

VERBATIM <sup>1</sup>RECORD OF TRIAL <sup>2</sup>

(and accompanying papers)

of

MANNING, Bradley E.

(Name: Last, First, Middle Initial)

[REDACTED]

(Social Security Number)

PFC/E-3

(Rank)

Headquarters and

Headquarters Company,

United States Army Garrison

(Unit/Command Name)

U.S. Army

(Branch of Service)

Fort Myer, VA 22211

(Station or Ship)

By

GENERALCOURT-MARTIAL

Convened by

Commander

(Title of Convening Authority)

UNITED STATES ARMY MILITARY DISTRICT OF WASHINGTON

(Unit/Command of Convening Authority)

Tried at

Fort Meade, MD

(Place or Places of Trial)

on

see below

(Date or Dates of Trial)

## Date or Dates of Trial:

23 February 2012, 15-16 March 2012, 24-26 April 2012, 6-8 June 2012, 25 June 2012, 16-19 July 2012, 28-30 August 2012, 2 October 2012, 12 October 2012, 17-18 October 2012, 7-8 November 2012, 27 November - 2 December 2012, 5-7 December 2012, 10-11 December 2012, 8-9 January 2013, 16 January 2013, 26 February - 1 March 2013, 8 March 2013, 10 April 2013, 7-8 May 2013, 21 May 2013, 3-5 June 2013, 10-12 June 2013, 17-18 June 2013, 25-28 June 2013, 1-2 July 2013, 8-10 July 2013, 15 July 2013, 18-19 July 2013, 25-26 July 2013, 28 July - 2 August 2013, 5-9 August 2013, 12-14 August 2013, 16 August 2013, and 19-21 August 2013.

<sup>1</sup> Insert "verbatim" or "summarized" as appropriate. (This form will be used by the Army and Navy for verbatim records of trial only.)

<sup>2</sup> See inside back cover for instructions as to preparation and arrangement.

damage assessment and all supporting documentation for an *in camera* review by the Court.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'David E. Coombs', with a stylized, flowing script.

DAVID EDWARD COOMBS  
Civilian Defense Counsel

# ATTACHMENT

## David Coombs

---

**From:** David Coombs <coombs@armycourt martialdefense.com>  
**Sent:** Saturday, April 21, 2012 11:15 AM  
**To:** 'Lind, Denise R COL MIL USA OTJAG'  
**Cc:** 'Tooman, Joshua J CPT USARMY (US)'; melissa.s.santiago.mil@mail.mil; 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; 'Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA'; 'Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA'; 'VonElten, Alexander S. 1LT USA JFHQ-NCR/MDW SJA'; 'Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA'; Ashden.Fein@jfhqncr.northcom.mil  
**Subject:** RE: Government Filings  
**Attachments:** Unclass Interim Assessments.pdf

Ma'am,

In the Government's Notification to the Court yesterday, it indicated that the Defense Intelligence Agency (DIA) and the Office of National Counterintelligence Executive (ONCIX) did not have any forensic results or investigative files related to this case.

Approximately a week ago, the Government produced to the Defense approximately 12 pages of Brady materials from interim damage assessments from November, 2010 by the Federal Communications Commission, the Federal Trade Commission, the U.S. Department of Urban Development, the Millennium Challenge Corporation, the National Archives, and the United States Marshals Service. [See Attached]. Some of these interim damage assessments reference investigations by ONCIX and DIA. For instance, the 26 November 2010 "Memorandum for the Office of the National Counterintelligence Executive (ONCIX)", the Federal Communications Commission states, "As requested, this Memorandum provides the response of the Federal Communications Commission (FCC), as requested by the NCIX memo dated 26 October 2010." (p. 1). Similarly, the 19 November 2010 letter from the U.S. Department of Housing and Urban Development is addressed to the DIA. Moreover, the DIA is overseeing the Information Review Task Force, an investigation into the alleged disclosures. Further, the interim damage assessments also reveal the Office of the Director of National Intelligence (ODNI) has relevant investigative files. See letter from United States Marshals ("On October 13, 2010, the Office of the Director of National Intelligence (ODNI) ... provided a checklist of questions that it recommended each agency impacted by [WL] dissemination use to assess the impact on its operations.") The Court's ruling did not specifically address ODNI; however, previous Defense requests for discovery asked the Government to provide all ODNI investigative files. The Defense will renew its discovery request for ODNI investigative files and forensic results based upon the interim damage assessments.

It is readily apparent that there are investigative files in the hands of the DIA, ONCIX and ODNI. The interim damage assessments clearly show this. Accordingly, the Defense does not understand how the Government can maintain that "DIA does not have any forensic results or investigative files" and "ONCIX does not have any forensic results or investigative files." The Defense requests that in light of the interim damage assessments, the Government provide a full explanation of its statement that neither of these agencies has investigative files and provide a witness from each of the relevant agencies to appear at a motions hearing.

v/r  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317



Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
[coombs@armycourt martialdefense.com](mailto:coombs@armycourt martialdefense.com)  
[www.armycourt martialdefense.com](http://www.armycourt martialdefense.com)

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

-----Original Message-----

From: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA [<mailto:Ashden.Fein@jfhqncr.northcom.mil>]  
Sent: Friday, April 20, 2012 6:26 PM  
To: Lind, Denise R COL MIL USA OTJAG  
Cc: David Coombs; Tooman, Joshua J CPT USARMY (US); [melissa.s.santiago.mil@mail.mil](mailto:melissa.s.santiago.mil@mail.mil); Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; VonElten, Alexander S. 1LT USA JFHQ-NCR/MDW SJA; Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA  
Subject: Government Filings

Ma'am,

Attached are the following filings:

1. Government Response to Court Discovery Order (Forensic Drives)
2. Government Proposed Case Calendar Explanation

As explained in the government's email on 17 April 2012, the United States notified the defense that we have offered to make forensic images of the operable drives available to the defense by 18 May 2012 in an effort to save time and resources for all parties involved (defense, government computer experts, government classification experts, and the Court). If the defense still requests forensic copies of the drives or access to the files, then we will voluntarily comply; however that will take additional time so that the security expert(s) can go through the individual files to determine their classification, as you will see from the numbers on the list and this list is only of those items searched for, and not all the documents and other files on the drives.

v/r  
MAJ Fein

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, xxx-xx- )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE MOTION TO  
RECORD AND TRANSCRIBE  
ALL R.C.M. 802 CONFERENCES**

2 June 2012

RELIEF SOUGHT

1. The Defense requests that this Court order that all future R.C.M. 802 conferences be recorded and transcribed for the record.

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. As the moving party, the Defense has the burden of persuasion. R.C.M. 905(c)(2)(A). The burden of proof is by a preponderance of the evidence. R.C.M. 905(c)(1).

EVIDENCE

3. The Defense does not request any witnesses or evidence be produced for this motion.

FACTS

4. On several occasions the parties have held R.C.M. 802 conferences in order to discuss case related issues. These conferences have mostly been held either in a conference room adjacent to the courtroom or by telephone when the parties are not centrally located.

5. The Court has discussed the content of the various R.C.M. 802 conferences on the record at the following Article 39(a) session. The Court has also invited the parties to add any detail either party desired to the Court's summary.

ARGUMENT

6. The Defense submits that this Court should order that all future 802 sessions be recorded and transcribed for the record for four reasons: (1) The Government often uses the 802 sessions to re-litigate matters already decided by the Military Judge under the auspices of “clarification”; (2) the Government often takes positions in 802 sessions which are inconsistent with its motions and what is says in open court; (3) the Government makes admissions in the 802 sessions which are relevant to the Defense’s discovery requests; and (4) there is sometimes confusion as to exactly what was said at the 802 session.

7. First, the Government has used the opportunity that the 802 sessions provide to re-litigate issues already decided by the Military Judge under the guise that it was simply “clarifying” something. For instance, in its 23 March 2012 Ruling, the Court ordered that the Government produce the Department of State damage assessment. Appellate Exhibit XXXVI. The Government then sought “clarification” as to what it had to produce, given that the Department of State “had not completed a damage assessment.” The Government then used that opportunity to argue that a draft damage assessment is not discoverable under *Giles* because it is speculative. Appellate Exhibit LXXI. Far from clarifying the Court’s ruling, the Government was attempting to take issue with it. This happened again during the latest 802 session. The Court once again ordered the Government to provide a Department of State witness to testify as to what documents the department had that were responsive to the Defense’s repeated discovery requests. The Government once again took this as an opportunity to re-litigate the issue, insisting that the Defense did not have the right to ask a Department of State witness questions about what they possess because this is a classic “fishing expedition.” Again, when the Government disagrees with the Court’s ruling, it simply asks for an 802 for “clarification.”

8. Second, the Government will often say something in an 802 session that is inconsistent with what it says in its motions and what it says in open court. In one 802 session, the Defense asked what material from the FBI file the Government intended to produce since its motion was unclear in this respect (and the Court had not ruled on this issue, given that the Government represented that it was in the process of producing all discoverable material). In the 802 session, the Government explained that some portions of the FBI file do not deal with PFC Manning at all – accordingly, those would not be produced. Everything else would be. In its subsequent motions and in open court, it changed its position and said that only *Brady* was discoverable from the FBI file. Similarly, the issue regarding ONCIX and “damage assessments” vs. “investigative” files was dealt with during an 802 session. The Government claimed that the Defense was using the wrong terminology in its discovery requests and that’s why it was not getting what it was looking for. Appellate Exhibit LXXII. Now, the Government is using the term “damage assessments” in the way that it told the Defense was incorrect. *See* Attachment. This Court and an appellate court should have the benefit of the Government’s shifting litigation positions.

9. Third, the Government makes admissions or statements during these 802 sessions that it later denies – which is made easier by the fact that there is no transcript of exactly what the Government said during that session. For instance, the Government said during the latest 802 conference that the requested Department of State materials were simply not discoverable under R.C.M. 701(a)(2) or R.C.M. 701(a)(6). The Defense asked how the Government could make this statement, given that it had not even reviewed the files? Now, it its Response to the Defense

Motion to Compel Discovery #2, it states at p. 2, "The prosecution has never stated that the defense is not entitled to any information discoverable under RCM 701(a)(6), and has consistently stated that the prosecution intends to review all documents for Brady and RCM 701(a)(6) material that is provided by the DoS that are responsive." Obviously, if the parties and the Court had a transcript of what was said, issues as to "who said what" could be easily resolved.

10. Fourth, there is sometimes confusion about what exactly was decided during the 802 session. At the latest 802 session, the Defense understood the Court to have ordered the Government to provide a list of all evidence it seeks to introduce in aggravation. The Government does not believe it needs to compile a list, but simply to give the Court a sense of the type of information it plans on introducing in aggravation. There was also some confusion on the dates when this needed to be produced. With the benefit of a transcript, both parties can have access to exactly what was decided at the 802 session.

11. As the Court is aware, there is a push for greater openness in this proceeding. At present, too many issues are being said and litigated behind closed doors. Accordingly, the Defense requests that this Court order a recording and transcript of all future 802 sessions.

#### CONCLUSION

12. The Defense requests that this Court order that all future R.C.M. 802 conferences be recorded and transcribed for the record.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

# ATTACHMENT



REPLY TO  
ATTENTION OF

DEPARTMENT OF THE ARMY  
U.S. ARMY MILITARY DISTRICT OF WASHINGTON  
210 A STREET  
FORT LESLEY J. MCNAIR, DC 20319-5013

ANJA-CL

30 May 2012

MEMORANDUM FOR Defense Counsel

SUBJECT: Disclosure of Damage Assessment, Department of Energy – United States v. PFC Bradley Manning

1. The Department of Energy has agreed to voluntarily disclose its damage assessment to the defense in classified discovery, rather than make it available for inspection, on the express condition that the accused shall not be given access to the document or the information contained therein. See Military Rule of Evidence 505(g)(1); see also Appellate Exhibit XXXII, para. 3(l)(7). The document is classified "SECRET//NOFORN."
2. Prior to releasing this document to the defense in classified discovery, all defense counsel shall sign, and return to the undersigned, the enclosure to this memorandum to acknowledge that the accused shall not be given access to the document or the information contained therein.
3. Upon receipt of all acknowledgments, the prosecution will immediately disclose this document (BATES 00449241-00449242).

J. HUNTER WHYTE  
CPT, JA  
Assistant Trial Counsel

Enclosure

Acknowledgement of Disclosure of Damage Assessment, Department of Energy

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

ORDER: DEPARTMENT  
OF STATE WITNESS FOR  
MOTIONS HEARING

4 June 2012

TO: Department of State

1. As the Military Judge presiding over the above-captioned General Court-Martial, I have determined, pursuant to Article 46, Uniform Code of Military Justice (10 U.S.C. § 846), Rule for Courts-Martial 701(g)(2) and (3), and Rule for Courts-Martial 703 that your organization has information which it is required to provide in the above referenced case.

2. You are directed to produce a witness or witnesses to testify as to the following subjects:

- a. The Chiefs of Mission review of the released cables at affected posts discussing their initial assessment;
- b. The WikiLeaks Working Group;
- c. The "Mitigation Team";
- d. The Department's reporting to Congress; and
- e. Group to Review Potential Risks to Individuals.

Additionally, the witness or witnesses are directed to testify whether the above referenced subjects had any documentation and in what form and whether any of this material is already contained within the damage assessment provided by the Department of State. See Supplement to Defense Motion to Compel Discovery #2, dated 30 May 2012, at 1.<sup>1</sup>

3. You will have the name(s) of the witness(es) to testify by 4 June 2012 and the witness(es) will be made available (in person or telephonically) for the motions hearing on 6-8 June 2012.

So ordered this 4th day of June 2012.



Denise R. Lind  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

<sup>1</sup> In the Supplement to Defense Motion to Compel Discovery #2, dated 30 May 2012, at 1, the defense grouped paragraphs 2(b) and 2(e) together; however, Ambassador Kennedy's testimony provided by the defense by email on 28 March 2012 references two separate subjects.

From: [Lind, Denise R COL USARMY \(US\)](#)  
To: [David Coombs](#)  
Cc: [Hurley, Thomas F MAJ USARMY \(US\)](#); [Tooman, Joshua J CPT USARMY \(US\)](#); [Santiago, Melissa S CW2 USARMY \(US\)](#); [Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA](#); [Overgaard, Angel M CPT USA JFHQ-NCR/MDW SJA](#); [Whyte, Jeffrey H CPT USA JFHQ-NCR/MDW SJA](#); [von Elten, Alexander S, CPT USA JFHQ-NCR/MDW SJA](#); [Ford, Arthur D CWA USA JFHQ-NCR/MDW SJA](#); [Williams, Patricia CIV JFHQ-NCR/MDW SJA](#); [Jefferson, Dashawn MSG USARMY \(US\)](#); [Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA](#)  
Subject: RE: Admin Issues (UNCLASSIFIED)  
Date: Tuesday, June 05, 2012 10:39:36 AM  
Attachments: [document2012-06-05-100912.pdf](#)

---

Classification: UNCLASSIFIED  
Caveats: NONE

Counsel,

Please find order attached. We will address the aggravation evidence from the Government on the record. The RCM 802 motion, although new, will also be addressed on 6 June 2012. We will also address the ONCIX issues. Group the DOS witnesses as close together as possible - Thursday afternoon/Friday.

Schedule the SCIF session Wed afternoon 1500 or later.

D

DENISE R. LIND  
COL, JA  
Chief Judge, 1st Judicial Circuit

-----Original Message-----

From: David Coombs [<mailto:coombs@armycourt martialdefense.com>]  
Sent: Monday, June 04, 2012 2:51 PM  
To: Lind, Denise R COL USARMY (US)  
Cc: Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US); Santiago, Melissa S CW2 USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Overgaard, Angel M CPT USARMY (US); Whyte, Jeffrey H CPT USARMY (US); 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; Ford, Arthur D Jr CW2 USARMY (US); Williams, Patricia A CIV (US); Jefferson, Dashawn MSG USARMY (US); Fein, Ashden MAJ USARMY (US)  
Subject: RE: Admin Issues

Ma'am,

In response to the Government's email:

1) Department of State: The Defense leaves it to your discretion to determine whether you think that the Government's proposed witnesses are appropriate. The Defense believes that producing three separate witnesses to testify at three separate times and who are knowledgeable with respect to only a limited slice of information from the Department of State is an attempt to frustrate the Court's order to produce one witness from the Department of State who has knowledge of the matters at issue. Additionally, the wording of the Government's proposed Court Order appears to attempt to limit the inquiry regarding the relevant topics.



2) SCIF: no issues

3) Aggravation Evidence: The Defense understood the Court's order in the 802 to be that the Government needed to provide a list of the actual aggravation evidence (not the general type of evidence) and that the submission was not to be ex parte.

4) Motions Hearing: There are two issues here: a) the 802 transcription request; b) the ONCIX motion.

a) Transcript: With respect to the 802 issue, this is a straightforward matter that does not require research on the Government's part. Either they oppose it or they don't. The Defense does not contemplate the need for oral argument on the issue. If we were to wait until the next motions hearing, this would defeat the whole purpose of the Defense's motion. Unless ordered to do so, the Defense does not wish to discuss any further substantive issues in the 802 sessions until the matter is resolved.

b) ONCIX: The Government has chosen to circumvent the requirement to motion the Court on when it needs to produce the damage assessment. The Government cannot unilaterally choose the day on which it wishes to produce a damage assessment and then claim, when the Defense requests immediate production, that this is the Defense's motion. In any event, the issue is straightforward and must be resolved as part and parcel of this round of discovery motions - or, as with the 802 issue, the Defense's motion is overcome by events. In other words, by delaying the litigation of these motions, the Government "wins" by default.

v/r,

David

David E. Coombs, Esq.

Law Office of David E. Coombs

11 South Angell Street, #317

Providence, RI 02906

Toll Free: 1-800-588-4156

Local: (508) 689-4616

Fax: (508) 689-9282

coombs@armycourtmartialdefense.com

www.armycourtmartialdefense.com

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

-----Original Message-----

From: Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA [<mailto:Ashden.Fein@jfhqncr.northcom.mil>]

Sent: Monday, June 04, 2012 2:11 PM

To: Lind, Denise R COL USARMY (US)

Cc: David Coombs; Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US); Santiago, Melissa S CW2 USARMY (US); Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA; Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA; Williams, Patricia CIV JFHQ-NCR/MDW SJA; Jefferson, Dashawn MSG USARMY (US)

Subject: Admin Issues

Ma'am,

The purpose of this email is to update the Court on current administrative issues, and it is unfortunately very lengthy:

I. Department of State Witnesses.

The Department of State requires a written order for witness production for the upcoming motions hearing. Attached is a proposed written order based on the defense's most recent supplemental filing.

Over the past four duty days, the Department has been working to identify witnesses to testify to the different subject matters. They have identified the following three witnesses:

- a. Ms. Catherine Brown, Deputy Assistant Secretary, Bureau of Intelligence and Research (INR), will testify for the limited purpose of the Chiefs of Mission cables and damage assessment.
- b. Ms. Marguerite Coffey, Former Director of the Office of Management Policy, Rightsizing and Innovation (M/PRI), will testify for the limited purpose of the mitigation team.

c. Ms. Rena Bitter, Director, Operations Center (S/ES-O), will testify for the limited purpose of the WikiLeaks working group and persons at risk working group.

Based on only having four duty days to identify the appropriate witnesses, the Department identified these individuals as being the most knowledgeable within the proposed scope AND available this week; however their availability on such short notice is limited. Ms. Brown is on leave all week, but can be available for telephonic testimony Thursday afternoon. Ms. Coffey and Ms.

Bitter are available for in-court testimony, but only as listed below, based on rearranging their schedules.

For testimony availability, the United States requests the Court take Ms.

Brown's testimony on Thursday afternoon, after 1400; Ms. Coffey's testimony on Wednesday (anytime) or Thursday morning; and Ms. Bitter's testimony starting after Friday afternoon.

2. SCIF Location. The government identified a SCIF conference room which can be used by the Court for the Article 39(a) session with the Court, Court Reporter, and government counsel. When does the Court want to meet for this Article 39(a), so that we can coordinate the time? The location is on Fort Meade and approximately 5 minutes from the courthouse by vehicle.

3. Government's Proposed Plan for Aggravation. The Government proposes that it submit to the Court a classified ex parte filing under RCM 701(g)(2) in order to provide the Court with an explanation of the types of information it intends to use as aggravation evidence in order to assist the Court in conducting its RCM 701 and MRE 505 reviews for discovery determinations.

Because this information is attorney work product, it should be submitted to the Court ex parte. Additionally, the Government intends to provide the Court with types of information that, although aggravating for presentencing purposes, the Government affirmatively acknowledges that it does not intend to present during presentencing proceedings through testimony or otherwise.

The Government proposes this information be due to the Court by COB, Friday 8 June 2012, so that the Government has adequate time to obtain approvals from equity holders of classified information to provide certain information to the Court.

4. This Motions Hearing Schedule. The government assumes the most recent defense motions (Defense Motion to Record and Transcribe all RCM 802 Conferences and Defense Motion on ONCIX Damage Assessment) will be placed on the Court Scheduling Order to be litigated in the next round of motions.

NOTE: Although the defense refers to their Motion on ONCIX Damage Assessment as a response, the government made no such motion. The government only gave notice of possible RCM 701(a)(6) material. The government is tracking the following motions being litigated this upcoming session:

a. Defense Motion to Compel Discovery #2 with Supplemental Filing b. Defense Motion for LIOs c. Defense Motion to ID Brady d. Defense Motion to Dismiss 793 Offenses c. Defense Motion to Dismiss 1030 Offenses f.

Government Motion for LIOs g. Case Scheduling Order

Next Session Scheduled for 16-20 July 2012 a. Defense Motion to Record RCM 802 Conferences b. Defense Motion on ONCIX Damage Assessment c. Government Motion to Reconsider Order: Government Motion: Protective Orders(s), dated 24 April 2012 d. Others Listed on Proposed Case Calendar

Thank you.

v/r

MAJ Fein

Classification: UNCLASSIFIED

Caveats: NONE

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, xxx-xx- )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**DEFENSE RESPONSE TO  
GOVERNMENT MOTION FOR  
APPROPRIATE RELIEF:  
PROPOSED LESSER-INCLUDED  
OFFENSES**

DATED: 23 May 2012

RELIEF SOUGHT

1. PFC Bradley E. Manning, by and through counsel, pursuant to applicable case law and Article 79, Uniform Code of Military Justice (UCMJ), 10 U.S.C. § 879 (2010), requests this Court to deny, in part,<sup>1</sup> the Government Motion for Proposed Lesser-Included Offenses (Government Motion).

BURDEN OF PERSUASION AND BURDEN OF PROOF

2. The Government, as the moving party, bears the burden of its motion by a preponderance of the evidence pursuant to R.C.M. 905(c)(1) and (2)(A).

WITNESSES/EVIDENCE

3. The Defense does not request any witnesses be produced for this motion. The Defense respectfully requests this court to consider the following evidence in support of the Defense's motion:

- a. Charge Sheet
- b. Army Regulation 380-5.
- c. Appellate Exhibit LXXX (Court's Ruling on Defense Motion to Dismiss Specification 1 of Charge II)

<sup>1</sup> The Defense concedes that under certain circumstances, attempt under Article 80, can be a lesser included offense (LIO) of the offenses charged in Specifications 2-16 of Charge II. The Defense does not believe attempt under Article 80 will qualify in this case. Additionally, the Defense concedes that a violation of 18 U.S.C. Section 641 with the value of the property being less than \$1,000 is a LIO of the offenses charged in Specifications 4, 6, 8, 12 and 16 of Charge II. Finally, the Defense also concedes that a violation of clause 1 and 2 of Article 134 is a LIO of the offenses charged in Specifications 13 and 14 of Charge II.

## LEGAL AUTHORITY AND ARGUMENT

4. The Government is not permitted to use clause 1 and 2 of Article 134 as a lesser included offense (LIO) of the violations of 18 U.S.C. Section 793(e) charged in Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II. The Government has identified in its motion the “act” that would constitute the first element of the clause 1 and 2 Article 134 offense as: “That the accused willfully communicated information related to the national defense.” Government Motion at 3; *see also* Charge Sheet (alleging this act). This act also constitutes a violation of Army Regulation 380-5 (AR 380-5), a punitive lawful general order in effect at the time of PFC Manning’s alleged actions. *See* Appellate Exhibit LXXX at 1. Where, as here, conduct is proscribed by a punitive lawful general order, the Government may not utilize clause 1 and 2 of Article 134 to punish that conduct; rather, the Government must charge that conduct as a violation of Article 92 or not at all. *See United States v. Borunda*, 67 M.J. 607, 609 (A.F. Ct. Crim. App. 2009).

5. The Government is also not permitted to utilize clause 1 and 2 of Article 134 to manufacture a larceny-type LIO of the violations of 18 U.S.C. Section 641 charged in Specifications 4, 6, 8, 12 and 16 of Charge II. Though the Government Motion does not identify with specificity the act that would constitute the first element of the clause 1 and 2 Article 134 LIO of the Section 641 violations, the language of Specifications 4, 6, 8, 12 and 16 of Charge II makes clear that the act for each specification is PFC Manning’s alleged obtainment of various computer databases or global address list owned by the Government under circumstances which make that obtainment a theft or knowing conversion of that database or global address list. *See* Charge Sheet. This larceny-type of offense must be charged under Article 121 or not at all; the preemption doctrine forbids the Government from using Article 134 to punish a larceny-type offense. *See United States v. Anderson*, 68 M.J. 378, 387 (C.A.A.F. 2010); *United States v. Kick*, 7 M.J. 82, 85 (C.M.A. 1979); *United States v. Wright*, 5 M.J. 106, 110-11 (C.M.A. 1978); *United States v. Norris*, 8 C.M.R. 36, 39-40 (C.M.A. 1953).

6. Therefore, this Court should deny the Government Motion insofar as it requests this Court to adopt the proposed clause 1 and 2 Article 134 LIOs for the violations of Section 793(e) and Section 641 alleged in Charge II.

### **A. The Government Cannot Use Clause 1 and 2 of Article 134 as a LIO of Violations of 18 U.S.C. Section 793(e)**

7. The Government cannot use clause 1 and 2 of Article 134 as a LIO of the violations of Section 793(e) charged in Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II. The act alleged in each of these specifications is proscribed by AR 380-5. Therefore, the act must be charged as a violation of Article 92 and cannot be charged as a violation of clause 1 and 2 of Article 134, as the Government has attempted to do with its proposed LIO. *See Borunda*, 67 M.J. at 609.

8. In Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II, PFC Manning is charged with violations of Section 793(e) under clause 3 of Article 134. *See* Charge Sheet. The Government has proposed a clause 1 and 2 Article 134 offense as a LIO of each of these Section 793(e)

violations. *See* Government Motion at 2. In general, conduct punished under clause 1 and 2 of Article 134 requires proof of the following elements:

- (1) That the accused did or failed to do certain acts; and
- (2) That, under the circumstances, the accused's conduct was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.

Manual for Courts-Martial (MCM), Part IV, para. 60.b. In this case, the Government has indicated in its motion that the act that would satisfy the first element of the clause 1 and 2 Article 134 offense is PFC Manning's willful communication of information related to the national defense. *See* Government Motion at 3. That same act is proscribed by AR 380-5, *see* AR 380-5, para. 1-21(a) ("DA personnel will be subject to sanctions if they knowingly, willfully, or negligently – (1) [d]isclose classified or sensitive information to unauthorized persons"), which is a punitive lawful general order that was in effect at the time of PFC Manning's alleged willful communication of information related to the national defense, *see* Appellate Exhibit LXXX at 1 ("At the time of PFC Manning's alleged unlawful actions, Army Regulation 380-5 (Department of the Army Information Security Program) was in effect. The regulation is a punitive lawful general order").

9. In *Borunda*, the Air Force Court of Criminal Appeals held that "when a lawful general order or regulation proscribing [certain conduct] exists, an order or regulation which by definition is punitive, the [proscribed conduct], if charged, will *only* survive legal scrutiny as a violation of Article 92(1), UCMJ, *and not as a violation* of Article 134, UCMJ." 67 M.J. at 609 (footnote omitted) (emphases supplied). Additionally, the MCM explains that "[m]any customs of the service are now set forth in regulations of the various armed forces. Violations of these customs *should be charged under Article 92* as violations of the regulations in which they appear if the regulation is punitive." MCM, Part IV, para. 60.c(2)(b) (emphasis supplied); *see* Appellate Exhibit LXXX at 4 ("Violations of customs of the service that are made punishable in punitive regulations should be charged under Article 92 as violations of the regulations in which they appear.").

10. After *Borunda*, it is clear that a court must not sustain a clause 1 and 2 Article 134 offense where the conduct underlying that offense also violates a lawful general order or regulation. This is precisely what the Government is requesting this Court to do with respect to the proposed clause 1 and 2 Article 134 LIO of the Section 793(e) violations.

11. In its Motion to Dismiss Specification 1 of Charge II for Failure to State an Offense (Defense Motion to Dismiss), the Defense raised a *Borunda* argument with respect to Specification 1 of Charge II, as the conduct underlying that specification was also proscribed by AR 380-5. This Court denied that motion, and it identified three reasons for doing so. *See* Appellate Exhibit LXXX at 5. First, Specification 1 of Charge II contained a different mens rea than AR 380-5: the specification included a wanton mens rea, whereas AR 380-5 requires a knowingly, willfully, or negligently mens rea. *Id.* Second, Specification 1 of Charge II contained an additional element not included in an AR 380-5 violation: that the accused knew

that intelligence published on the internet is accessible to the enemy. *Id.* Finally, the term “intelligence” included information that does not fall within AR 380-5’s prohibition on the disclosure of classified or sensitive information. *Id.* For all of these reasons, this Court determined that the situation was “distinct from *Borunda*, as that case addressed an Article 134 specification where the offense charged was specifically proscribed in a punitive regulation.” *Id.*

12. None of these three reasons identified by this Court in Appellate Exhibit LXXX are implicated in this instance. In fact, each reason militates in favor of the conclusion that the Government’s proposed clause 1 and 2 Article 134 LIO of the Section 793(e) offenses runs afoul of *Borunda*.

13. First, the act that would constitute the first element of the proposed clause 1 and 2 Article 134 LIO – the *willful* communication of information relating to the national defense, *see* Government Motion at 3 – has a *mens rea* that is included in AR 380-5’s *mens rea* requirement, *see* AR 380-5 (punishing anyone who knowingly, *willfully*, or negligently discloses classified or sensitive information). Second, unlike Specification 1 of Charge II, the clause 1 and 2 Article 134 offense does not contain an element in addition to the *willful* communication of information relating to the national defense.<sup>2</sup> The only act constituting the purported Article 134 violation is the *willful* communication of information relating to the national defense. That act is “specifically proscribed in a punitive regulation.” Appellate Exhibit LXXX at 5. Finally, while the scope of the term “relating to the national defense” is not free from doubt, *see* Defense Motion to Dismiss Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II at 3-4, 7-8, the specific information identified in Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II is clearly classified or sensitive information within AR 380-5. As this Court has observed:

AR 380-5 defines classified information as “information and material that has been determined, pursuant to [Executive Order] 12958 or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary and readable form.” Sensitive information but unclassified information is defined as “information originated from within the Department of State which warrants a degree of protection and administrative control and meets the criteria for exemption from mandatory public disclosure under the Freedom of Information Act.”

Appellate Exhibit LXXX at 2 (quoting AR 380-5). The information identified in Specifications 3, 5, 7, 9, 10 and 15 of Charge II is expressly alleged to be classified. *See* Charge Sheet. Additionally, it seems apparent that the information in Specifications 2 and 11 of Charge II,

---

<sup>2</sup> To be sure, the proposed clause 1 and 2 Article 134 LIO does contain the element that the conduct of the accused was to the prejudice of good order and discipline in the armed forces and of a nature as to bring discredit upon the armed forces. *See* MCM, Part IV, para. 60.b. But that is true in all cases where a clause 1 and 2 Article 134 offense is alleged. It was certainly true in *Borunda*, where the accused was charged under clause 1 and 2 of Article 134 for wrongful possession of drug paraphernalia. *See* 67 M.J. at 608-09. This did not prevent the *Borunda* Court from holding, in no uncertain terms, that “when a lawful general order or regulation proscribing [certain conduct] exists, an order or regulation which by definition is punitive, the [proscribed conduct], if charged, will only survive legal scrutiny as a violation of Article 92(1), UCMJ, and not as a violation of Article 134, UCMJ.” *Id.* at 609 (footnote omitted). Thus, this additional element in a clause 1 and 2 Article 134 offense is entirely irrelevant to the *Borunda* inquiry.



though not expressly alleged to be classified, meets either AR 380-5's definition of "classified information" or its definition of "sensitive information." *See id.* Thus, it cannot be said, as it could for the term "intelligence" in Specification 1 of Charge II, that the "information relating to the national defense" identified in Specifications 2, 3, 5, 7, 9, 10, 11 and 15 is beyond the scope of AR 380-5. On the contrary, AR 380-5 squarely prohibits the disclosure of the information identified in these specifications.

14. Therefore, as none of the three important reasons this Court identified for its denial of the Defense Motion to Dismiss are present in this case, *Borunda* forbids the Government from using clause 1 and 2 of Article 134 as a LIO for the Section 793(e) offenses, when the "act" that would form the first element of the clause 1 and 2 Article 134 LIO is a breach of a custom set forth in a punitive regulation. Thus, the Court should deny the Government's request that it adopt a clause 1 and 2 Article 134 LIO for Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II.

**B. The Government Cannot Use Clause 1 and 2 of Article 134 as a LIO of Violations of 18 U.S.C. Section 641**

15. The Government cannot utilize clause 1 and 2 of Article 134 to manufacture a LIO of the violations of Section 641. The act constituting the first element of the purported clause 1 and 2 Article 134 LIO would be a larceny-type act. The preemption doctrine forbids the Government from using Article 134 to create new larceny-type offenses that do not fall within, or have not been charged under, Article 121.

16. In Specifications 4, 6, 8, 12 and 16 of Charge II, PFC Manning is charged with violations of Section 641 under clause 3 of Article 134. *See* Charge Sheet. The Government has proposed a clause 1 and 2 Article 134 LIO for each of these offenses. *See* Government Motion at 2. As mentioned above, conduct punished under clause 1 and 2 of Article 134 requires proof of the following elements:

- (1) That the accused did or failed to do certain acts; and
- (2) That, under the circumstances, the accused's conduct was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.

MCM, Part IV, para. 60.b. In this case, the Government has not indicated in its motion what the act or acts are that establish the first element of the clause 1 and 2 Article 134 offense. But from the language of Specifications 4, 6, 8, 19 and 16 of Charge II, it seems clear that the acts are PFC Manning's alleged obtaining of various computer databases and a global address list owned by the Government under circumstances which make that obtaining a theft or knowing conversion of that database and global address list. *See* Charge Sheet.

17. This is a larceny-type offense. Article 121 punishes both larceny and wrongful appropriation. *See* 10 U.S.C. § 921. It provides, in pertinent part, as follows:

Any person subject to this chapter who wrongfully takes, obtains, or withholds, by any means, from the possession of the owner or of any other person any money, personal property, or article of value of any kind --

(1) with intent permanently to deprive or defraud another person of the use and benefit of property or to appropriate it to his own use or the use of any person other than the owner, steals that property and is guilty of larceny; or

(2) with intent temporarily to deprive or defraud another person of the use and benefit of property or to appropriate it to his own use or the use of any person other than the owner, is guilty of wrongful appropriation.

*Id.* § 921(a). Notably, the Government elected not to charge PFC Manning's alleged unlawful obtainment of the various databases and global address list identified in Specifications 4, 6, 8, 12 and 16 of Charge II as violations of Article 121. Instead, the Government chose to charge these alleged unlawful actions as violations of Section 641. The preemption doctrine prevents the Government from using Article 134 as a purported LIO to punish a larceny-type offense when it elected not to utilize Article 121 in the first place.

18. The then-Court of Military Appeals has defined the doctrine of preemption as “the legal concept that where Congress has occupied the field of a given type of misconduct by addressing it in one of the specific punitive articles of the code, another offense may not be created and punished under Article 134, UCMJ, simply by deleting a vital element.” *Kick*, 7 M.J. at 85. The preemption doctrine is described in paragraph 60.c(5)(a) of the MCM as follows:

The preemption doctrine prohibits application of Article 134 to conduct covered by Articles 80 through 132. For example, larceny is covered in Article 121, and if an element of that offense is lacking – for example, intent – there can be no larceny or larceny-type offense, either under Article 121 or, because of preemption, under Article 134. *Article 134 cannot be used to create a new kind of larceny offense, one without the required intent, where Congress has already set the minimum requirements for such an offense in Article 121.*

MCM, Part IV, para. 60.c(5)(a) (emphases supplied). Courts apply a two-pronged test to determine whether an Article 134 charge is preempted by another Article in any given case. First, it must be shown that Congress “indicate[d] through direct legislative language or express legislative history that particular actions or facts are limited to the express language of an enumerated article, and may not be charged under Article 134, UCMJ.” *Anderson*, 68 M.J. at 387; *see Kick*, 7 M.J. at 85; *Wright*, 5 M.J. at 110-11; *see also* Appellate Exhibit LXXX at 2 (explaining this prong). Second, it must be established that the offense charged under Article 134 is composed of a “residuum of elements” of an enumerated offense under the UCMJ. *Wright*, 5 M.J. at 111; *see Kick*, 7 M.J. at 85; *see also* Appellate Exhibit LXXX at 2-3 (explaining this prong).

19. The Court of Military Appeals in *Norris* squarely addressed the issue of whether Article 134 may be used to create a larceny-type offense, as the Government seeks to do in the present case

with its purported clause 1 and 2 Article 134 LIO. In *Norris*, the accused was charged with larceny and wrongful appropriation under Article 121 and wrongful taking under Article 134. 8 C.M.R. at 37-38. The accused was initially found guilty of wrongful appropriation and wrongful taking, but on appeal the board of review held that the law officer had erred in not instructing on the effect of intoxication on specific intent. *Id.* at 38. The board remedied this defect by vacating the wrongful appropriation conviction and affirming the wrongful taking conviction under Article 134, as the offenses charged under Article 121 required a specific intent to deprive the owner of the property, either permanently or temporarily, and the wrongful taking charge required only a general criminal intent. *Id.* The Court of Military Appeals reversed, holding that “there is no offense known as ‘wrongful taking’ requiring no element of specific intent, embraced by Article 134 of the Code.” *Id.* at 40. The Court reasoned that:

Article 134 should generally be limited to military offenses and those crimes not specifically delineated by the punitive articles . . . . We cannot grant to the services unlimited authority to eliminate vital elements from common law crimes and offenses expressly defined by Congress and permit the remaining elements to be punished as an offense under Article 134.

*Id.* at 39.

20. The *Norris* Court readily found the requisite congressional intent that Article 121 govern the universe of larceny-type offenses under the UCMJ: “Congress has, in Article 121, covered the entire field of criminal conversion for military law.” *Id.* As for the second prong, the *Norris* Court found that the wrongful taking offense charged under Article 134 was composed of a residuum of elements of wrongful appropriation under Article 121; the wrongful taking offense had all of the elements of a wrongful conversion except for the specific intent element. *Id.* at 38-39.

21. Just as the Government was not permitted in *Norris* to use Article 134 to create a larceny-type offense when it was unable to prove the requisite intent under Article 121, so too should the Government not be permitted here to use Article 134 to create a larceny-type offense as a LIO of a federal theft and conversion statute. *See id.* at 39-40; *see also* MCM, Part IV, para. 60(c)(5)(a). Congress “covered the entire field of criminal conversion for military law” in Article 121. *Norris*, 8 C.M.R. at 39. The Government chose not to utilize Article 121 in this case. Moreover, the clause 1 and 2 Article 134 LIO would be composed of a residuum of Article 121 larceny-type elements. The alleged unlawful acts, though not expressly identified in the Government Motion, are the obtainment of databases and a global address list under circumstances which constitute a theft or knowing conversion. At a minimum, the Government will have to prove a larceny-type intent (intent to permanently or temporarily deprive the Government of the use and benefit of the databases and global address list) and a larceny-type act (the obtainment of the databases and global address list). *See* MCM, Part IV, para. 46.b (outlining elements of larceny and wrongful appropriation under Article 121). Thus, both prongs of the preemption doctrine are satisfied by the Government’s proposed clause 1 and 2 Article 134 LIO.


22. Therefore, because the preemption doctrine forbids the Government from using Article 134 to punish a larceny-type offense, the Government may not utilize clause 1 and 2 of Article 134 to

manufacture a LIO of Section 641 in this case. Thus, the Court should deny the Government's request that it adopt a clause 1 and 2 Article 134 LIO for Specifications 4, 6, 8, 12 and 16 of Charge II.

CONCLUSION

23. For these reasons, the Defense requests that this Court deny, in part, the Government Motion.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC  
U.S. Army, xxx-xx-  
Headquarters and Headquarters Company,  
U.S. Army Garrison, Joint Base Myer-  
Henderson Hall, Fort Myer, VA 22211

)  
)  
) **RULING: GOVERNMENT  
MOTION FOR EXTENSION  
OF TIME TO RESPOND TO  
DEFENSE 505(g)(2) MOTION**

)  
)  
)  
)  
)  
) **DATED: 24 May 2012**

1. On 18 May 2012, the Government made disclosures to the Court and provided notice of intent IAW MRE 505(g)(2) to file *ex parte* motions for the Court to conduct an *in camera* review and authorized a substitution of the classified DIA Information Review Task Force (IRT) Final Report and a substitution for the classified WikiLeaks task Force report.
2. On 22 May 2012, Defense filed a motion requesting the Court order the Government to provide non *ex parte* version of its motion pursuant to MRE 505(i). This motion was not on the Court's scheduling calendar for the 6-8 June 2012 motions.
3. On 22 May 2012, via email, the Court ordered the Government to respond by 24 May 2012. Also via email, the Government requested leave of court to respond by 29 May 2012. On 23 May 2012, the Court granted the Government request via email and also extended the deadline for the Defense to respond to the Government's disclosures until 1 June 2012.
4. On 23 May 2012, the Court ordered the Government to put their email request in a motion. On 23 May, the Government filed a motion for leave to respond by 29 May 2012. Also on 23 May 2012, the Defense filed a request opposing the motion.
5. The Court's *in camera* review of the DIA Information Review Task Force (IRT) Final Report and the WikiLeaks task force report will not be stayed.

**RULING:** The Court modifies its email grant of the Government's request for an extension of time to respond as follows: (1) Government response is due by COB 28 May 2012. (2) The Court will rule on the Defense motion on 29 May 2012. (3) Should the Court rule in favor of the Defense, the Government will give the Defense a non *ex parte* version of its motion on 30 May 2012. The Defense response to the Government motion is due on 1 June 2012. Issues regarding the DIA Information Review Task Force (IRT) Final Report and the WikiLeaks task force report will be addressed at the Article 39(a) session 6-8 June 2012.

**ORDERED** this 24<sup>th</sup> day of May 2012.



DENISE R. LIND  
COL., JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

UNITED STATES OF AMERICA )

v. )

Prosecution Disclosure  
to the Court

Manning, Bradley E. )

PFC, U.S. Army, )

HHC, U.S. Army Garrison, )

Joint Base Myer-Henderson Hall )

Fort Myer, Virginia 22211 )

18 May 2012

1. On 23 March 2012, the Court ordered the prosecution as follows:

a. The Government will immediately begin the process of producing the damage assessments that are outside the possession, custody, or control of military authorities IAW RCM 703(f)(4)(A). If necessary, the Government shall prepare an order for the Court to sign for each custodian.

b. The Government shall contact Department of State (DOS), Federal Bureau of Investigation (FBI), Defense Intelligence Agency (DIA), Office of the National Counterintelligence Executive (ONCIX), and Central Intelligence Agency (CIA) to determine whether these agencies contain any forensic results or investigative files relevant to this case. The Government will notify the court NLT 20 April 2012 whether any such files exist. If they do exist, the Government will examine them for evidence that is favorable to the accused and material to either guilt or punishment.

c. By 20 April 2012, the Government will notify the Court with a status of whether it anticipates any government entity that is the custodian of classified evidence that is the subject of the Defense Motion to Compel will seek limited disclosure IAW MRE 505(g)(2) or claim a privilege IAW MRE 505(c) for the classification under that agency's control.

d. By 18 May 2012, the Government will disclose any unclassified information from the 3 damage assessments that is favorable to the accused and material to guilt or punishment and provide any additional unclassified information from the damage assessments to the Court for *in camera* review IAW RCM 701(g)(2).

e. By 18 May 2012, the Government will identify what classified information from the 3 damage reports it found that was favorable to the accused and material to guilt or punishment. By 18 May 2012, the Government will disclose all classified information from the 3 damage assessments to the Court for *in camera* review IAW RCM 701(g)(2) or, at the request of the Government, *in camera* review for limited disclosure under MRE 505(g)(2).

f. By 18 May 2012, if the relevant Government agency claims a privilege under MRE 505(c) and the Government seeks an *in camera* proceeding under MRE 505(i), the Government will move for an *in camera* proceeding IAW MRE 505(i)(2) and (3) and provide notice to the Defense under MRE 505(i)(4)(A).

2. On 16 April 2012, the Court granted the Government's motion for leave of the Court to extend the time to respond from 20 April 2012 to 2 May 2012 as to whether the CIA will release classified information in original form, provide for limited disclosure under MRE 505(g)(2), or invoke the classified information privilege under MRE 505(c).

3. On 20 April 2012, the United States notified the Court of the following:

a. The prosecution contacted the DOS, FBI, CIA, DIA, and ONCIX to determine whether these agencies contain any forensic results or investigative files relevant to this case.

(1) **DOS.** DOS has forensic results and investigative files. The United States reviewed this information for evidence that is favorable to the accused and material to either guilt or punishment. Additionally, prior to the Court's order, the United States produced this information to the defense.

(2) **FBI.** FBI has forensic results and investigative files. The United States is reviewing this information for evidence that is favorable to the accused and material to either guilt or punishment. Additionally, prior to the Court's order, the United States started producing this information to the defense.

(3) **DIA.** DIA does not have any forensic results or investigative files.

(4) **ONCIX.** ONCIX does not have any forensic results or investigative files.

b. The United States anticipates that the **FBI** is the only government entity that is a custodian of classified forensic results or investigative files relevant to this case that will seek limited disclosure IAW MRE 505(g)(2).

4. On 2 May 2012, the United States notified the Court of the following:

a. The prosecution contacted the CIA to determine whether this agency contains any forensic results or investigative files relevant to this case.

**CIA.** The CIA has investigative files. The United States reviewed this information for evidence that is favorable to the accused and material to either guilt or punishment.

b. The United States anticipates that the **FBI** and **CIA** are the only government entities that are custodians of classified forensic results or investigative files relevant to this case that will seek limited disclosure IAW MRE 505(g)(2).

5. On 11 May 2012, the Court denied the Government's Motion to find the DOS Draft Damage Assessment not discoverable.

## 6. Forensic Results or Investigative Files.

a. **FBI.** The United States completed its review of the FBI investigative file for evidence that is favorable to the accused and material to either guilt or punishment.<sup>1</sup> On 16 March 2012, and immediately following the Court's issuing of the classified information protective order, the United States started voluntarily disclosing information from the FBI file, including information favorable to the accused and material to either guilt or punishment under MRE 505(g)(1). Except for twenty-two documents, as of the date of this response, the United States has voluntarily produced all information (unclassified or classified) under MRE 505(g)(1). The twenty-two remaining documents will be delivered to the defense on 21 May 2012 under MRE 505(g)(1).

b. **CIA.** The United States completed its review of the CIA forensic results or investigative files for evidence that is favorable to the accused and material to either guilt or punishment.<sup>2</sup> Any information (unclassified or classified) the prosecution identified will be voluntarily produced under MRE 505(g)(1) and delivered to the defense on 21 May 2012.

## 7. Damage Assessments.

a. **DOS.** The DOS provided the prosecution a copy of the draft DOS damage assessment to make available for the defense to inspect in a government facility under MRE 505(g)(1). *Sec* Enclosure. The copy does not contain redactions or summaries. The DOS authorizes only defense counsel and their security experts to inspect the document. The accused is not authorized to inspect or receive any information contained within the document. The prosecution requests the defense provide four duty days notice before each time they would like to inspect the document, so that the proper facility and government security expert may be made available.

b. **DIA.** The United States completed its review of the DIA Information Review Task Force (IRTF) Final Report for evidence that is favorable to the accused and material to either guilt or punishment. The United States also reviewed the document for information material to the preparation of the defense because DIA is an intelligence agency within the Department of Defense. Concurrent with this response, the United States is filing *ex parte* a Government *in camera* Motion for Authorization of a Substitution under MRE 505(g)(2). This motion directly responds to whether the United States identified any information that was favorable to the accused and material to guilt or punishment and includes a copy of the original damage assessment and an alternate version. Additionally, the motion outlines other equity holders outside of military authorities that request certain redactions or summaries of their information. If the Court authorizes the substitutions under MRE 505(g)(2), then DIA and other equity holders are not invoking the classified information privilege under MRE 505(c) and MRE 505(i), and the alternative copy of the Final Report will be made available to the defense for inspection

<sup>1</sup> The United States understands its continuing obligation to review the FBI forensic results or investigative files until this court-martial is complete.

<sup>2</sup> The United States understands its continuing obligation to review the CIA forensic results or investigative files until this court-martial is complete.



at DIA under MRE 505(g)(1) and MRE 505(g)(2). This alternative copy includes any unclassified information that is responsive to the Court's Order. DIA authorizes only defense counsel and their security experts to inspect the document at DIA, and requires the security experts to be present with defense counsel. The accused is not authorized to inspect or receive any information contained within the document.

c. **CIA.** The United States completed its review of the WikiLeaks Task Force report for evidence that is favorable to the accused and material to either guilt or punishment. The United States did not identify any unclassified information that was responsive to the Court's Order. Concurrent with this response, the United States is filing *ex parte* a Government *in camera* Motion for Authorization of a Substitution under MRE 505(g)(2). This motion directly responds to whether the United States identified any information that was favorable to the accused and material to guilt or punishment and includes a copy of the original report and an alternative version, if required. If the Court authorizes the substitutions under MRE 505(g)(2), the CIA is not invoking the classified information privilege under MRE 505(c) and MRE 505(i).



ASHDEN FEIN  
MAJ, JA  
Trial Counsel

Enclosure

Letter from DOS, dated 18 May 2012, without attachment (Sensitive but Unclassified without Attachment)



United States Department of State

*The Legal Adviser*

*Washington, D.C. 20520*

SECRET//NOFORN

(SENSITIVE BUT UNCLASSIFIED when separated from enclosure)

May 18, 2012

Major Ashden Fein  
Trial Counsel, Criminal Law Division  
Office of the Staff Judge Advocate  
Department of the Army

*Re: United States v. Private First Class Bradley E. Manning*

Dear Major Fein:

Enclosed please find a draft document entitled "WikiLeaks: Foreign Policy Impact of the Net-Centric Diplomacy Compromise" ("the draft"). The draft document is classified "Secret//Noform" (i.e., Secret and not to be shared with foreign nationals), and is the same as was provided under cover of our April 25, 2012 letter, except that we have now placed a watermark of the word "DRAFT" on each page of the draft document, whereas the previous version we provided only had this watermark on the cover page.

Pursuant to the Court's orders dated May 11, 2012 and March 23, 2012 in the above referenced matter, we are providing you this draft document to allow defense counsel to inspect the draft inside a government facility as part of classified discovery. Additionally, we authorize the defense Security Experts, referred to in paragraph 3(f) (page 3) of the Court's March 16, 2012 Protective Order for Classified Information, to inspect the draft, as required by them to perform their functions in this case. We do not authorize the defendant to inspect the draft, nor do we authorize defense counsel to convey the substance of classified information contained in the draft to the defendant.

SECRET//NOFORN

(Sensitive But Unclassified when separated from attachment)

SECRET//NOFORN

(Sensitive But Unclassified when separated from attachment)

- 2 -

We have not declassified the draft document, nor do we anticipate doing so within the timeframe that this case may proceed to trial. As such, the document remains classified "Secret//Noform" (i.e., Secret and not to be shared with foreign nationals). We understand that all defense counsel have a security clearance and have signed a Standard Form 312 Classified Information Nondisclosure Agreement (SF 312) and a protective order, and as such are bound to safeguard and handle the enclosed draft in accordance with Executive Order (EO) 13526 and the CAPCO standards, as well as the requirements reflected in SF 312 and the Court's protective order. We understand that defense counsel will be allowed to take notes; however, any notes of classified information will themselves be classified and will also be safeguarded and handled appropriately consistent with EO 13526 and the CAPCO standards, as well as the requirements reflected in SF 312 and the Court's protective order.

We do not object to this letter being shared with the Court or defense counsel.

Very truly yours,

A handwritten signature in blue ink, appearing to read "Richard C. Visek", written over a horizontal line.

Richard C. Visek  
Deputy Legal Adviser

Enclosure: As stated

SECRET//NOFORN

(Sensitive But Unclassified when separated from attachment)

## UNITED STATES

 $\gamma$ 

**MANNING, Bradley E., PFC**  
**U.S. Army, xxx-xx-xxxx**  
**Headquarters and Headquarters Company, U.S.**  
**Army Garrison, Joint Base Myer-Henderson Hall,**  
**Fort Myer, VA 22211**

**RULING: GOVERNMENT:  
MOTION FOR  
CONTINUANCE**

**31 May 2012**

**RULING:** The Government motion for a continuance until 31 May 2012 is **GRANTED**.

**ORDERED:** This 31st day of May 2012.

DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

Prosecution Request  
for Additional Time to Supplement  
Court Order to Provide Unclassified and  
Redacted Version of Government  
*Ex-Parte* Filing

30 May 2012

1. The United States requests additional time to supplement its response to the Court's Order to provide the Court and the defense with an unclassified and redacted version of its Defense Intelligence Agency (DIA) *ex-parte* filing (hereinafter "DIA *ex-parte* filing"), dated 18 May 2012, until 31 May 2012.
2. At 1652 hours on 29 May 2012, the Court ordered, via email, the United States to "provide the Court and the Defense with an unclassified redacted version of its *ex-parte* motion NLT 30 May 2012 that describes the general nature of the proposed substitutions and the national security interest the Government seeks to protect with the substitutions." See Ruling: Defense Motion: Non-Ex Parte Filing by Government, dated 29 May 2012. The United States complied with the Court's Order by contemporaneously filing the Prosecution's Disclosure to the Defense, dated 30 May 2012, along with the unclassified and redacted versions of its *ex-parte* filings.
3. By 1900 hours tonight, the United States obtained approval from all but one federal organization with equity in the DIA damage assessment to release an unclassified and redacted version of the DIA *ex-parte* filing. The United States coordinated to obtain approval from the remaining federal organization with equity in the DIA damage assessment by contacting, throughout the day, three separate attorneys at the organization. The primary and alternate attorneys assigned to handle this case were out of the office for the entire day. In an effort to exhaust all possible resources, the United States contacted a third attorney, who is not assigned to this case and who responded at approximately 1900 hours tonight. This attorney attempted to contact an original classification authority (OCA) to review the Government's proposed redactions of classified information, but no OCA was available to assist.
4. Although the United States has provided the defense an unclassified and redacted version of the DIA *ex-parte* filing, the United States requests one additional duty day to supplement its response to the Court's Order. The United States intends to receive approval from the government organization to provide the defense a less redacted copy of the DIA *ex-parte* filing, as well as a possibly more detailed unclassified explanation of the national security interests the Government seeks to protect with the limited disclosure. This request will not necessitate any delay in the proceedings and will potentially disclose even more information to the defense; as such, there will be no prejudice to the defense.

  
ASHDEN FEIN  
MAJ, JA  
Trial Counsel

(127)

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 30 May 2012.

A handwritten signature in black ink, appearing to read 'ASHDEN FEIN', with a stylized, flowing script.

ASHDEN FEIN  
MAJ, JA  
Trial Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, xxx-xx- )

Headquarters and Headquarters Company, )

U.S. Army Garrison, Joint Base Myer- )

Henderson Hall, Fort Myer, VA 22211 )

**RULING: DEFENSE MOTION  
TO COMPEL DISCOVERY -  
DAMAGE ASSESSMENTS - DOS,  
DIA IRTF, CIA.**

DATED: 6 June 2012

On 23 March 2012, the Court ordered the Government by 18 May 2012 to disclose damage assessments by the DIA Information Review Task Force (IRTF), the Department of State (DOS), and the Central Intelligence Agency (CIA) to the Court for *in camera* review in accordance with (IAW) RCM 701(g)(2).

On 18 April 2012, the Defense moved the Court to find that the above damage assessments are in the possession, custody, and control of military authorities and discoverable as material to the preparation of the Defense IAW RCM 701(a)(2).

On 26 April 2012, the Government requested the Court reconsider its ruling with respect to the State Department damage assessment because the assessment is a draft and, therefore, not discoverable.

On 11 May 2012, the Court denied the Government's motion.

On 18 May 2012, the Government filed two classified *ex parte* motions with the Court to authorize redactions for the DIA IRTF final report and the CIA WikiLeaks Task Force report.

On 22 May 2012, the Defense moved the Court to order the Government to provide a non *ex parte* version of its motions and proceed under MRE 505(i).

On 29 May 2012, the Court granted the Defense motion in part.

On 1 June 2012 the Defense filed its Response to the Government Motions for authorization of a substitution and asked the Court to consider the following factors when conducting its 505(g)(2) *in camera* reviews:

- a) What is the extent of the redactions/substitutions?
- b) Has the Government narrowly tailored the substitutions to protect a Governmental interest that has been clearly and specifically articulated?
- c) Does the substitution provide the Defense with the ability to follow-up on leads that the original document would have provided?

- d) Do the substitutions accurately capture the information within the original document?
- e) Is the classified evidence necessary to rebut an element of the 22 charged offenses, bearing in mind the Government's very broad reading of many of these offenses?
- f) Does the summary strip away the Defense's ability to accurately portray the nature of the charged leaks?
- g) Do the substitutions prevent the Defense from fully examining witnesses?
- h) Do the substitutions prevent the Defense from exploring all viable avenues for impeachment?
- i) Does the Government intend to use any of the information from the damage assessments? Is so, is this information limited to the summarized document provided by the Government? If the information intended to be used by the Government is not limited to the summarized document, does the Defense in fairness need to receive the classified portions of the documents to put the Government's evidence in proper context?
- j) Does the original classified evidence present a more compelling sentencing case than the proposed substitutions by the Government?
- k) Do the proposed substitutions prevent the Defense from learning names of potential witnesses?
- l) Do the substitutions make sense, such that the Defense will be able to understand the context?
- m) Is the original classified evidence necessary to help the Defense in formulating defense strategy and making important litigation decisions in the case?
- n) Is it unfair that the Government had access to the unclassified version of the damage assessment and the Defense did not? Does that provide a tactical advantage to the Government?

After considering the pleadings, evidence presented, and argument of counsel, and after conducting *in camera* review of the DIA IRTF final report and the CIA WikiLeaks task force report considering the factors requested by the Defense, the Court finds and concludes the following:

**1. DOS Damage Assessment:** On or about 18 April 2012, the Government produced the DOS draft damage assessment to the Court for *in camera* review and requested reconsideration of its 23 March 2012 order. On 11 May 2012, the Court denied the Government's request for reconsideration. On 18 May 2012, the Government advised the Court that the Government would produce the draft report without redaction to Defense Counsel and their security experts. As such, the Defense motion to compel the DOS damage assessment and to find it discoverable under RCM 701(a)(2) is moot.

**2. DIA Information Review Task Force (IRTF).** On 18 May 2012, the Government produced the IRTF final report to the Court for *in camera* review and a substituted final report with proposed redactions IAW MRE 505(g)(2). The Court conducted an *in camera* review of the original IRTF final report and the proposed substitution considering the factors requested by the Defense and finds:

a. Whether evaluating the substitutions under RCM 701(a)(6) or RCM 701(a)(2), the redacted substitution is sufficient for the Defense to adequately prepare for trial and represent an appropriate balance between the right of the Defense to discovery and the protection of specific



national security information. The redactions are minor and limited in scope. The Government is releasing the report almost in its entirety.

b. The redactions are not favorable to the accused; material to the preparation of the defense; or necessary to enable the accused to prepare for trial.

c. Each of the redactions constitutes specific classified information. Redaction is necessary to protect national security and particular sources and methods.

The Government will disclose the redacted DIA IRTF final report to the defense by COB today. The Defense Motion to Compel the DIA IRTF final report is moot.

3. **CIA.** The Government completed a review of the CIA WikiLeaks Task Force report for evidence favorable to the accused and material to guilt or punishment. The Government filed an *ex parte* motion for *in camera* review by the Court IAW MRE 505(g)(2) to determine whether a proposed Government substitution shall be disclosed to the Defense or whether disclosure of the classified information itself is necessary to enable the accused to prepare for trial. The Court has conducted an *in camera* review of the classified information considering the factors requested by the Defense. The Government substitute discloses *Brady* and RCM 701(a)(6) material but not material under RCM 701(a)(2). The Court does not find at this time that the proposed substitute is sufficient. The Court will meet *ex parte* with Government counsel in an area appropriate for review of classified information. A court reporter will transcribe the classified proceedings.

**RULING:** The Classified motions by the Government to voluntarily provide limited disclosure under MRE 505(g)(2) of the DIA IRTF final report is **GRANTED**. The Court finds the substitution as currently drafted is not sufficient under MRE 505(g)(2) and holds the decision in abeyance pending the *ex parte* proceeding with the Government and review of what the Government intends to introduce and not introduce in its sentencing case.



DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, xxx-xx- )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**RULING: DEFENSE MOTION -  
RECORD AND TRANSCRIBE  
RCM 802 CONFERENCES**

DATED: 6 June 2012

Defense moves the Court to order all RCM 802 conferences be recorded and transcribed for the record. The Government opposes. After considering the pleadings, evidence presented, and argument of counsel, the Court finds and concludes the following:

1. The trial schedule developed by the Court and the parties provides for Article 39(a) sessions to be held approximately every 5-6 weeks. To date, there have been Article 39(a) sessions held on 23 February, 15-16 March, 24-26 April, and the current session from 4-6 June 2012.
2. RCM 802 provides that after referral, the military judge may, upon request of either party or *sua sponte*, order one or more conferences with the parties to consider such matters as will promote a fair and expeditious trial. Conferences need not be made part of the record, but matters agreed upon at a conference shall be included in the record orally or in writing. Failure of a party to object at trial to failure to comply with RCM 802 waives this requirement. No party may be prevented from making any argument, objection, or motion at trial. The discussion to the rule states that the purposes of RCM 802 conferences is to inform the military judge of anticipated issues and to expeditiously resolve matters on which the parties can agree, not to litigate or decide contested issues.
3. The Court has been holding RCM 802 conferences with counsel during and following the Article 39(a) sessions and by telephone on 8 February 2012, 28 March 2012, and 30 May 2012. Each of these conferences have been synopsisized on the record, and the Court has invited the parties to add detail to the Court's synopsis.
4. Prior to the current motion dated 2 June 2012, the Defense has not objected to conducting RCM 802 conferences.
5. RCM 802 does not require that such conferences be recorded and transcribed. The Court will continue to hold such conferences with the parties to address administrative, logistics, and scheduling issues. If either party objects to discussion of an issue in an RCM 802 conference,

the conference will be terminated and the issue will be addressed at the next Article 39(a) session.

6. The Court notes that the parties have raised substantive issues in the middle of Article 39(a) scheduling periods that, if not addressed expeditiously, will delay the trial. Therefore, the Court, in conjunction with the parties, will build in an additional Article 39(a) session into the Court calendar approximately midway in between in each scheduled Article 39(a) session to address such issues that arise. If additional substantive issues arise that require expeditious resolution, the Court, will schedule additional *ad hoc* Article 39(a) sessions as necessary.

**RULING:**

1. The Defense Motion to Record and Transcribe RCM 802 conferences is **DENIED**.
2. RCM 802 conferences will not be held over the objection of a party.
3. The Court will schedule an additional Article 39(a) session in between currently scheduled sessions to address on the record any additional issues that arise in between scheduled sessions.

**So Ordered** this 6<sup>th</sup> day of June 2012.



DENISE R. LIND  
COL., JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

Appellate Exhibit 130  
151 pages  
ordered sealed for Reason 5  
Military Judge's Seal Order  
dated 20 August 2013  
stored in the original Record  
of Trial

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, xxx-xx- )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**RULING: DEFENSE MOTION -  
COMPEL IDENTIFICATION OF  
BRADY MATERIALS**

DATED: 7 June 2012

Defense moves the Court to exercise its inherent discretion and order the Government to identify or separate *Brady* material<sup>1</sup> when providing discovery to the Defense. The Government opposes. After considering the pleadings, evidence presented, and argument of counsel, the Court finds and concludes the following:

1. Defense asserts the Government has provided the Defense with twelve (12) pages of *Brady* material taken from an assessment/investigation/working document review by the Office of the National Counterintelligence executive (ONCIX), Office of the Director of National Intelligence (ODNI), and the Information Review Task Force (IRTF) of the Defense Intelligence Agency (DIA). Additionally, the Government has provided the Defense with approximately 9,000 pages, from the Federal Bureau of Investigation ("FBI"), which contain *Brady* material and additional discovery. The pages are redacted. Defense asserts the FBI files are not text searchable.
2. There are 4 available facilities where the Defense can store and access the FBI files: (1) Trial Defense Office, Fort Myer, VA – available since 12 October 2010; (2) Trial Defense Office, Fort Leavenworth (TDS) – available since 22 June 2011; (3) Trial Defense Office, Fort Meade, MD – available since 10 August 2011; and (4) Naval War College, Rhode Island, approximately 30 miles from Mr. Coombs' office. At the request of Civilian Defense Counsel (CDC), Mr. Coombs, the Government provided facilities in Rhode Island to make it easier for him to access and store classified information without having to travel to the National Capital Region.
3. There are currently 3 Defense Counsel representing the accused: Mr. Coombs, CDC, MAJ Hurley, Individual Military Counsel (IMC), and CPT Tooman (detailed defense counsel). The accused released his original detailed defense counsel, MAJ Kemkes and CPT Bouchard, during the Article 39(a) session on 15-16 March 2012. CPT Tooman was detailed to the case during the Article 39(a) session 24-26 April 2012 and MAJ Hurley was added to the Defense team as Individual Military Counsel on 6 June 2012 during the current Article 39(a) session. Defense has not requested additional staffing for the defense team.

<sup>1</sup> *Brady v. Maryland*, 373 U.S. 83 (1963).

4. The Accused is in pretrial confinement at Fort Leavenworth, Kansas. There is a safe to store classified information at the Fort Leavenworth trial defense office.

5. The parties dispute whether the Government is required to release the non-*Brady* portions of the FBI file under RCM 702(a)(2) as material to the preparation of the defense. The bulk of the FBI discovery given by the Government to the Defense thus far is *Brady* material. There is no evidence that the Government has "padded the file" or otherwise exercised bad faith in burying the *Brady* needle in the haystack of FBI files disclosed.

6. Neither RCM 701(a)(6) nor *Brady* require the Government to identify or separate what material it discloses in discovery is *Brady* material. See *U.S. v. Warshak*, 631 F.3d 266 (6<sup>th</sup> Cir. 2010) (declining to order the Government to organize and index discovery when not required by Federal Rule of Criminal Procedure 16). The Court has not been presented with any military cases addressing this issue, however, the Court agrees with the 5<sup>th</sup> Circuit that there is no general duty that requires the Government to direct the Defense to exculpatory evidence within a larger mass of disclosed evidence. *U.S. v. Skilling*, 554 F.3d 529, 576 (5<sup>th</sup> Cir. 2009).

7. Defense relies primarily on *U.S. v. Salyer*, 2010 WL 3036444 (E.D.Cal. 2010); and *U.S. v. Hsia*, 24 F.Supp.2d 14 (D.D.C. 1998). Both of those cases involved "open file" cases with far more voluminous discovery than at issue in this case and, in each, there was evidence that the prosecution dumped the haystack of discovery requiring the Defense to find the *Brady* needle. In *Salyer*, the Court accepted the general rule set forth in *Skilling* and *Warshack*, but, as a matter of case management, ordered the Government to identify *Brady* material from what the Court described as a massive amount of documentary information collected over 5 years consisting of multiple gigabytes, pages numbering in the millions, and hardcopy information filling more than 2 "pods" (storage containers).

8. Discovery is voluminous in this case, but not nearly to the extent as in *Salyer* or *Hsia*. To date, the Government has provided the Defense with more than 43,886 documents consisting of 411,366 pages. The approximately 9,000 pages the Defense alleges has been disclosed from the redacted FBI files are a small part of the total discovery to date. There is no evidence that the Government is padding discovery to hide *Brady* material.

9. The Court finds no good cause to deviate from the general rule that the Government is not required to sift through each item of discovery and separate or identify *Brady* information contained within a larger mass of disclosed evidence.

**RULING:** The Defense Motion to Compel Identification of *Brady* material is **Denied**.



DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

Appellate Exhibit 132

5 pages

classified

"SECRET"

ordered sealed for Reason 2

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

Appellate Exhibit 132

Enclosure 1

122 pages

classified

"SECRET"

ordered sealed for Reason 2  
and Reason 7 (government)

Military Judge's Seal Order

dated 20 August 2013

stored in the classified  
supplement to the original  
Record of Trial



Appellate Exhibit 132

Enclosure 2

123 pages

classified

"SECRET"

ordered sealed for Reason 2  
and Reason 7 (government)

Military Judge's Seal Order

dated 20 August 2013

stored in the classified  
supplement to the original  
Record of Trial

Appellate Exhibit 132

Enclosure 3

3 pages

classified

"SECRET"

ordered sealed for Reason 2  
and Reason 7 (government)

Military Judge's Seal Order

dated 20 August 2013

stored in the classified  
supplement to the original  
Record of Trial

Appellate Exhibit 132

Enclosure 4

5 pages

classified

"SECRET"

ordered sealed for Reason 2  
and Reason 7 (government)

Military Judge's Seal Order  
dated 20 August 2013

stored in the classified  
supplement to the original  
Record of Trial

Appellate Exhibit 132

Enclosure 5

5 pages

classified

"SECRET"

ordered sealed for Reason 2  
and Reason 7 (government)

Military Judge's Seal Order  
dated 20 August 2013

stored in the classified  
supplement to the original  
Record of Trial

Appellate Exhibit 133

3 pages

classified

"SECRET"

ordered sealed for Reason 2  
and Reason 7 (government)

Military Judge's Seal Order  
dated 20 August 2013

stored in the classified  
supplement to the original  
Record of Trial

Appellate Exhibit 133

Enclosure 1

classified

"TOP SECRET"

ordered sealed for Reason 1

and Reason 7 (government)

Military Judge's Seal Order

dated 20 August 2013

is stored at the Office of the

General Counsel, Central

Intelligence Agency pursuant

to AE 500

Appellate Exhibit 133

Enclosure 2

classified

"SECRET//HCS"

ordered sealed for Reason 1  
and Reason 7 (government)

Military Judge's Seal Order  
dated 20 August 2013

is stored at the Office of the  
General Counsel, Central  
Intelligence Agency pursuant  
to AE 500

Appellate Exhibit 133

Enclosure 3

4 pages

classified

"SECRET"

ordered sealed for Reason 2  
and Reason 7 (government)

Military Judge's Seal Order

dated 20 August 2013

stored in the classified  
supplement to the original

Record of Trial



Westlaw.

S. REP. 99-432

Page 1

S. Rep. No. 432, 99TH Cong., 2ND Sess. 1986, 1986 U.S.C.A.N. 2479, 1986 WL 31918, S. REP. 99-432 (Leg.Hist.)

**\*2479 P.L. 99-474, COMPUTER FRAUD AND ABUSE ACT OF 1986  
DATES OF CONSIDERATION AND PASSAGE**

House June 3, October 6, 1986

Senate October 1, 3, 1986

House Report (Judiciary Committee) No. 99-612,

May 22, 1986 [To accompany H.R. 4718]

Senate Report (Judiciary Committee) No. 99-432,

Sept. 3, 1986 [To accompany S. 2281]

Cong. Record Vol. 132 (1986)

The House bill was passed in lieu of the Senate bill after amending its language to contain much of the text of the Senate bill. The Senate Report is set out below.

**SENATE REPORT NO. 99-432**

September 3, 1986

The Committee on the Judiciary, to which was referred the bill (S. 2281) to amend title 18, United States Code, to provide additional penalties for fraud and related activities in connection with access devices and computers, and for other purposes, having considered the same, reports favorably thereon with amendments and recommends that the bill, as amended, do pass.

\*\*\*\*\*

**I. GENERAL STATEMENT AND HISTORY OF THE LEGISLATION**

During the past several years, the Congress has been investigating the problems of computer fraud and abuse to determine whether Federal criminal laws should be revised to cope more effectively with such acts. The Judiciary Committee's concern about these problems has become more pronounced as computers proliferate in businesses and homes across the nation and as evidence mounts that existing criminal laws are insufficient to address the problem of computer crime.

For some time, the United States has been in the midst of a technological explosion. The Federal Government alone operates more than 18,000 medium-scale and large-scale computers at some 4,500 different sites, and the Office of Technology Assessment estimates the Government's investment in computers over the past four years at roughly \$60 billion. The General Services Administration estimates that there will be 250,000 to 500,000 computers in use by the Federal Government by 1990.

Computer use has also become much more widespread among the nation's private sector. In 1978, there were an estimated 5,000 desk-top computers in this country; today there are nearly 5 million. Financial institutions, in particular, rely heavily on computer \*2480 communications; for instance, the Bureau of Justice Statistics reported that in 1983, corporate transfers of funds via computer totaled more than \$100 trillion.<sup>1</sup> In addition, more than 100,000 personal computers have been installed in the country's schools, and computers are found in millions of American homes.

This technological explosion has made the computer a mainstay of our communications system, and it has brought a great many benefits to the government, to American businesses, and to all of our lives. But it has also

created a new type of criminal—one who uses computers to steal, to defraud, and to abuse the property of others. The proliferation of computers and computer data has spread before the nation's criminals a vast array of property that, in many cases, is wholly unprotected against crime.

In June 1984, the American Bar Association Task Force on Computer Crime, chaired by Joseph Tompkins, Jr., issued its Report on Computer Crime (hereinafter referred to as the 'ABA Report'), a study based upon a survey of approximately 1,000 private organizations and public agencies.<sup>2</sup> The ABA Report found that more than 50 percent of the 283 respondents had been victimized by some form of computer crime,<sup>3</sup> and that more than 25 percent of the respondents had sustained financial losses totaling between an estimated \$145 million and \$730 million during one twelve-month period.<sup>4</sup> The ABA Report also concluded that computer crime is among the worst white-collar offenses.<sup>5</sup> The Committee agrees but notes particularly that computer crimes pose a threat that is not solely financial in nature.

In 1983, for example, a group of adolescents known as the '414 Gang' broke into the computer system at Memorial Sloan-Kettering Cancer Center in New York. In so doing, they gained access to the radiation treatment records of 6,000 past and present cancer patients and had at their fingertips the ability to alter the radiation treatment levels that each patient received. No financial losses were at stake in this case, but the potentially life-threatening nature of such mischief is a source of serious concern to the Committee.

Similarly, so-called 'pirate bulletin boards' have sprung up around the country for the sole purpose of exchanging passwords to other people's computer systems. The *Richmond (Va.) Times-Dispatch* recently reported that three such bulletin boards operating in Virginia carry information on how to break into the computers of the U.S. Defense Department and the Republican National Committee. While financial losses resulting from such pirate bulletin boards may not be imminent, the Committee believes that knowingly trafficking in other people's computer passwords should be proscribed.

It is clear that much computer crime can be prevented by those who are potential targets of such conduct. The ABA Report indicated that while the respondents to the survey overwhelmingly supported<sup>6</sup> a Federal computer crime statute,<sup>7</sup> they also believed that the most effective means of preventing and deterring computer crime is 'more comprehensive and effective self-protection by private business' and that the primary responsibility for controlling the incidence of computer crime falls upon private industry and individual users, rather than on the Federal, State, or local governments.<sup>8</sup> The Committee strongly agrees with these views.

The Committee also finds that education programs for both computer users and the general public should be undertaken to make young people and others aware of the ethical and legal questions at stake in the use of computers and to deflate the myth that computer crimes are glamorous, harmless pranks. The respondents to the ABA survey indicated strong support for such programs,<sup>9</sup> many of which are underway throughout the nation. The Committee commends those education and security improvement efforts and urges their continuation.

At the same time, the Committee finds that Federal criminal penalties for computer crime are an appropriate punishment for certain acts and can serve to deter would-be computer criminals and to reinforce education and security improvement programs.

To that end, both the Senate and House have devoted considerable attention to determining how the Federal Government can best approach computer-related crimes. The first Federal computer crime statute was enacted in 1984 as part of P.L. 98-473. This is the present 18 U.S.C. 1030, which makes it a felony to access classified information in a computer without authorization and makes it a misdemeanor to access financial records or credit histories in financial institutions or to trespass into a Government computer.

Legislation was introduced in both the Senate and House early in the 99th Congress to expand and to amend 18 U.S.C. 1030. On May 23, 1985, the House Subcommittee on Crime held a hearing on H.R. 1001 (introduced by Representative William J. Hughes (D-N.J.) and H.R. 930 (introduced by Representative Bill Nelson (D-Fla.)). Representative Bill McCollum, R-Fla., subsequently introduced a computer crime bill, H.R. 3381, at the request

of the Department of Justice. The Senate Subcommittee on Criminal Law held a hearing on October 30, 1985, on two computer crime bills: S. 440 (introduced by Senator Paul Trible (R-Va.) and S. 1678 (introduced by Senator Strom Thurmond, (R-S.C., at the request of the Department of Justice). S. 1678 is the Senate companion to H.R. 3381.

As a result of the testimony given at both the Senate and House hearings, Senator Trible and Representative Hughes introduced identical computer crime bills (S. 2281 and H.R. 4562) on April 10, 1986. The House Subcommittee on Crime considered H.R. 4562 on April 23, and on April 30 the subcommittee forwarded a clean bill, H.R. 4718, to the Committee on the Judiciary in lieu of H.R. 4562. The Committee on the Judiciary ordered H.R. 4718, as amended, reported on May 6 (see House Report 99-612), and on June 3 the House passed the bill by voice vote. In the Senate, the Committee on the Judiciary held a hearing on S. 2281 on April 16, 1986. The \*2482 Committee ordered the bill, as amended, reported to the Senate on June 12, 1986.

Throughout its consideration of computer crime, the Committee has been especially concerned about the appropriate scope of Federal jurisdiction in this area. It has been suggested that, because some States lack comprehensive computer crime statutes of their own, the Congress should enact as sweeping a Federal statute as possible so that no computer crime is potentially uncovered. The Committee rejects this approach and prefers instead to limit Federal jurisdiction over computer crime to those cases in which there is a compelling Federal interest, i.e., where computers of the Federal Government or certain financial institutions are involved, or where the crime itself is interstate in nature. The Committee is convinced that this approach strikes the appropriate balance between the Federal Government's interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses.

S. 2281, as reported by the Committee, is a consensus bill aimed at deterring and punishing certain 'high-tech' crimes in a manner consistent with the States' own criminal laws in this area.

## II. DISCUSSION OF COMMITTEE ACTION AND AMENDMENTS

On June 12, 1986, the Committee on the Judiciary met and unanimously ordered S. 2281 reported favorably to the full Senate. Several minor amendments were also approved unanimously by the Committee.

The first amendment was a technical change to page two, line eight of the bill, made necessary because of the second Committee amendment. That second amendment struck lines 9-24, relating to unauthorized access of Government computers, on page two, and inserted in their place the language that forms the new subsection 18 U.S.C. 1030(a)(3), as reported. That subsection is explained in detail in the section-by-section analysis of this Report.

The third Committee amendment struck the new subsection (a)(5) from S. 2281 as introduced, and replaced it with amended language. In so doing the Committee added to (a)(5) the words 'damages, or destroys' to make explicit the subsection's application to acts—such as erasing data—that go beyond mere alteration of information. This amendment also changed 'that computer' (as written in the original S. 2281) to 'any such Federal interest computer'. The Committee wanted to prevent the possibility that a defense would be raised to the effect that the information that was altered, damaged, or destroyed, was not in the very same computer on to which the offender had signed. The use of 'any such Federal interest computer' makes clear that no such defense is possible. This amendment also deleted 'another' from the portion of S. 2281 relating to subsection (a)(5); the phrase 'one or more others' was inserted in its place. The Committee does not intend that every victim of acts proscribed under (a)(5) must individually suffer a loss of \$1,000. Certain types of malicious mischief may cause smaller amounts of damages to numerous individuals, and thereby collectively create a loss of more than \$1,000. By using 'one or more \*2483 others', the Committee intends to make clear that losses caused by the same act may be aggregated for purposes of meeting the \$1,000 threshold. Finally, this amendment added to the coverage of the new

subsection (a)(5) acts that alter, damage, or destroy computerized medical records, and thereby impair or threaten to impair an individual's medical care. The Committee's rationale for this addition is explained more fully in the section-by-section analysis pertaining to the new 18 U.S.C. 1030(a)(5).

The fourth Committee amendment changed 'such use' to 'the use of the financial institution's operation or the Government's operation of such computer'. This change simply makes clear that a computer that is not used exclusively by the United States Government or by a financial institution, as that term is defined by proposed 18 U.S.C. 1030(e)(4), is a Federal interest computer only to the extent that its use by the Government or the financial institution is affected. This clarification also appears in the Committee's amendment affecting proposed 18 U.S.C. 1030(a)(3).

The fifth Committee amendment was merely a technical change made necessary because the sixth Committee amendment added 'department of the United States' to the list of terms defined in the bill.

### III. SECTION-BY-SECTION ANALYSIS

The following is a section-by-section analysis of S. 2281, as reported by the Committee on the Judiciary.

Section 1 of the bill contains its short title, the 'Computer Fraud and Abuse Act of 1986'.

Section 2(a)(1) amends 18 U.S.C. 1030(a)(2) to change the scienter requirement from 'knowingly' to 'intentionally', for two reasons. First, intentional acts of unauthorized access—rather than mistaken, inadvertent, or careless ones—are precisely what the Committee intends to proscribe. Second, the Committee is concerned that the 'knowingly' standard in the existing statute might be inappropriate for cases involving computer technology. The Senate's Report on the Criminal Code (Report No. 96-1396, pg. 33, citing *United States v. United States Gypsum Co.*, 438 U.S. 422, 425\* (1978)), states that a person is 'said to act knowingly if he is aware 'that the result is practically certain to follow from his conduct, whatever his desire may be as to that result.' (Footnote omitted.) While appropriate to many criminal statutes, this standard might not be sufficient to preclude liability on the part of those who inadvertently 'stumble into' someone else's computer file or computer data. This is particularly true in those cases where an individual is authorized to sign onto and use a particular computer, but subsequently exceeds his authorized access by mistakenly entering another computer file or data that happens to be accessible from the same terminal. Because the user had 'knowingly' signed onto that terminal in the first place, the danger exists that he might incur liability for his mistaken access to another file. This is so because, while he may not have desired that result, i.e., the access of another\*2484 file, it is possible that a trier of fact will infer that the user was 'practically certain' such mistaken access could result from his initial decision to access the computer. The substitution of an 'intentional' standard is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another. Again, this will comport with the Senate Report on the Criminal Code, which states that "intentional" means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective." (Footnote omitted.)

Section 2(a)(2) deletes from the existing 18 U.S.C. 1030(a)(2) the phrase 'as such terms are defined in the Right to Financial Privacy Act of 1978 (12 U.S.C. 3401 et seq.)'. The terms to which that phrase is applicable, 'financial institution' and 'financial record,' are defined in section 2(g) of S. 2281.

The premise of 18 U.S.C. 1030(a)(2) will remain the protection, for privacy reasons, of computerized credit records and computerized information relating to customers' relationships with financial institutions. This protection is imperative in light of the sensitive and personal financial information contained in such computer files. However, by referring to the Right to Financial Privacy Act, the current statute limits its coverage to financial institution customers who are individuals, or are partnerships with five or fewer partners. The Committee intends S. 2281 to extend the same privacy protections to the financial records of all customers—individual, part-

nership, or corporate—of financial institutions.

The Department of Justice has expressed concerns that the term 'obtains information' in 18 U.S.C. 1030(a)(2) makes that subsection more than an unauthorized access offense, i.e., that it might require the prosecution to prove asportation of the data in question.<sup>10</sup> Because the premise of this subsection is privacy protection, the Committee wishes to make clear that 'obtaining information' in this context includes mere observation of the data. Actual asportation, in the sense of physically removing the data from its original location or transcribing the data, need not be proved in order to establish a violation of this subsection.

Section 2(b) of S. 2281 provides a substitute for the present 18 U.S.C. 1030(a)(3), and is designed to accomplish several goals.

First, it will change the scienter requirement from 'knowingly' to 'intentionally'. The same explanation offered for section 2(a)(1) is applicable here.

Second, section 2(b) will clarify the present 18 U.S.C. 1030(a)(3), making clear that it applies to acts of simple trespass against computers belonging to, or being used by or for, the Federal Government. The Department of Justice and others have expressed concerns about whether the present subsection covers acts of mere trespass, i.e., unauthorized access, or whether it requires a further showing that the information perused was 'used, modified, destroyed, or disclosed.'<sup>11</sup> To alleviate those concerns, the Committee<sup>2485</sup> wants to make clear that the new subsection will be a simple trespass offense, applicable to persons without authorized access to Federal computers.

The Committee wishes to be very precise about who may be prosecuted under the new subsection (a)(3). The Committee was concerned that a Federal computer crime statute not be so broad as to create a risk that government employees and others who are authorized to use a Federal Government computer would face prosecution for acts of computer access and use that, while technically wrong, should not rise to the level of criminal conduct. At the same time, the Committee was required to balance its concern for Federal employees and other authorized users against the legitimate need to protect Government computers against abuse by 'outsiders.' The Committee struck that balance in the following manner.

In the first place, the Committee has declined to criminalize acts in which the offending employee merely 'exceeds authorized access' to computers in his own department ('department' is defined in section 2(g) of S. 2281). It is not difficult to envision an employee or other individual who, while authorized to use a particular computer in one department, briefly exceeds his authorized access and peruses data belonging to the department that he is not supposed to look at. This is especially true where the department in question lacks a clear method of delineating which individuals are authorized to access certain of its data. The Committee believes that administrative sanctions are more appropriate than criminal punishment in such a case. The Committee wishes to avoid the danger that every time an employee exceeds his authorized access to his department's computers—no matter how slightly—he could be prosecuted under this subsection. That danger will be prevented by not including 'exceeds authorized access' as part of this subsection's offense.

In the second place, the Committee has distinguished between acts of unauthorized access that occur within a department and those that involve trespasses into computers belonging to another department. The former are not covered by subsection (a)(3); the latter are. Again, it is not difficult to envision an individual who, while authorized to use certain computers in one department, is not authorized to use them all. The danger existed that S. 2281, as originally introduced, might cover every employee who happens to sit down, within his department, at a computer terminal which he is not officially authorized to use. These acts can also be best handled by administrative sanctions, rather than by criminal punishment. To that end, the Committee has constructed its amended version of (a)(3) to prevent prosecution of those who, while authorized to use some computers in their department, use others for which they lack the proper authorization. By precluding liability in purely 'insider' cases such as these, the Committee also seeks to alleviate concerns raised by Senators Mathias and Leahy that the ex-

isting statute casts a wide net over 'whistleblowers,' who disclose information they have gleaned from a government computer. Senators Mathias and Leahy first expressed their concerns in 1984 \*2486 about the effect of the current statute on whistleblowers. Their concerns were embodied in S. 610, a bill they introduced early in the 99th Congress. (See, Statements by Senator Mathias and Senator Leahy, Congressional Record of March 7, 1985; pp. S 2728-2730. See also their 'Additional Views' in this report.)

The Committee has thus limited 18 U.S.C. 1030(a)(3) to cases where the offender is completely outside the Government, and has no authority to access a computer of any agency or department of the United States, or where the offender's act of trespass is interdepartmental in nature. The Committee does not intend to preclude prosecution under this subsection if, for example, a Labor Department employee authorized to use Labor's computers accesses without authorization an FBI computer. An employee who uses his department's computer and, without authorization, forges into data belonging to another department, is engaged in conduct directly analogous to an 'outsider' tampering with Government computers. In both cases, the user is wholly lacking in authority to access or use that department's computer. The Committee believes criminal prosecution should be available in such cases.

The Committee acknowledges that in rare circumstances this may leave serious cases of intradepartmental trespass free from criminal prosecution under (a)(3). However, the Committee notes that such serious acts may be subject to other criminal penalties if, for example, they violate trade secrets laws or 18 U.S.C. 1030(a)(1), (a)(4), (a)(5), or (a)(6), as proposed in this legislation. The Committee believes this to be the best means of balancing the legitimate need to protect the Government's computers against the need to prevent unwarranted prosecutions of Federal employees and others authorized to use Federal computers.

The third goal of Section 2(b) is to clarify subsection (a)(3) to make clear that one trespassing in a computer used only part-time by the Federal Government need not be shown to have affected the operation of the government as a whole. The Department of Justice has expressed concerns that the present subsection's language could be construed to require a showing that the offender's conduct harmed the overall operation of the Government and that this would be an exceedingly difficult task for Federal prosecutors.<sup>12</sup> Accordingly, Section 2(b) will make clear that the offender's conduct need only affect the use of the Government's operation of the computer in question.

Section 2(c) substitutes the phrase 'exceeds authorized access' for the more cumbersome phrase in present 18 U.S.C. 1030(a)(1) and (a)(2), 'or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend'. The Committee intends this change to simplify the language in 18 U.S.C. 1030(a)(1) and (2), and the phrase 'exceeds authorized access' is defined separately in Section 2(g) of the bill.

Section 2(d) adds three new offenses to 18 U.S.C. 1030. The new subsection 1030(a)(4) to be created by this bill is designed to penalize thefts of property via computer that occur as part of a scheme \*2487 to defraud. It will require a showing that the use of the computer or computers in question was integral to the intended fraud and was not merely incidental. It has been suggested that the Committee approach all computer fraud in a manner that directly tracks the existing mail fraud and wire fraud statutes. However, the Committee was concerned that such an approach might permit prosecution under this subsection of acts that do not deserve classification as 'computer fraud.'

The Committee was concerned that computer usage that is wholly extraneous to an intended fraud might nevertheless be covered by this subsection if the subsection were patterned directly after the current mail fraud and wire fraud laws. If it were so patterned, the subsection might be construed as covering an individual who had devised a scheme or artifice to defraud solely because he used a computer to keep records or to add up his potential 'take' from the crime. The Committee does not believe that a scheme or artifice to defraud should fall under the ambit of subsection (a)(4) merely because the offender signed onto a computer at some point near to the com-

mission or execution of the fraud. While such a tenuous link might be covered under current law where the instrumentality used is the mails or the wires, the Committee does not consider that link sufficient with respect to computers. To be prosecuted under this subsection, the use of the computer must be more directly linked to the intended fraud. That is, it must be used by an offender without authorization or in excess of his authorization to obtain property of another, which property furthers the intended fraud. Likewise, this subsection may be triggered by conduct that can be shown to constitute an attempted offense.

This approach is designed, in part, to help distinguish between acts of theft via computer and acts of computer trespass. In intentionally trespassing into someone else's computer files, the offender obtains at the very least information as to how to break into that computer system. If that is all he obtains, the offense should properly be treated as a simple trespass. But because the offender has obtained the small bit of information needed to get into the computer system, the danger exists that his and every other computer trespass could be treated as a theft, punishable as a felony under this subsection. A similar problem arises from recommendations made to the Committee that every act of unauthorized access to a 'Federal interest computer' be treated as theft of computer time, punishable under this subsection as part of a scheme to defraud. The Committee agrees that the mere use of a computer or computer service has a value all its own. Mere trespasses onto someone else's computer system can cost the system provider a 'port' or access channel that he might otherwise be making available for a fee to an authorized user. At the same time, the Committee believes it is important to distinguish clearly between acts of fraud under (a)(4), punishable as felonies, and acts of simple trespass, punishable in the first instance as misdemeanors. That distinction would be wiped out were the Committee to treat every trespass as an attempt to defraud a service provider of computer time. One simply cannot trespass into another's computer without occupying a portion of the time that that computer service is available. Thus, \*2488 that suggested approach would treat every act of unauthorized entry to a Federal interest computer—no matter how brief—as an act of fraud, punishable at the felony level. The Committee does not believe this is a proper approach to this problem. For that reason, the Committee has excluded from coverage under this subsection those instances where 'the object of the fraud and the thing obtained consists only of the use of the computer.'

However, the Committee agrees that lost computer time resulting from repeated or sustained trespasses can reach a level of seriousness sufficient to warrant Federal prosecution. The Committee believes such instances are more appropriately punished under the provision of the new subsection (a)(5) relating to preventing authorized use of a computer. A more detailed explanation of the Committee's intent respecting lost computer time is contained in the analysis for (a)(5).

The Committee remains convinced that there must be a clear distinction between computer theft, punishable as a felony, and computer trespass, punishable in the first instance as a misdemeanor. The element in the new paragraph (a)(4), requiring a showing of an intent to defraud, is meant to preserve that distinction, as is the requirement that the property wrongfully obtained via computer furthers the intended fraud. The new felony created by this subsection limits its jurisdiction to 'Federal interest computers.' These are defined in Section (2)(g) of the bill as computers used by the Federal Government or by financial institutions, or as computers located in different States.

The scienter requirement for this subsection, 'knowingly and with intent to defraud,' is the same as the standard used for 18 U.S.C. 1029 relating to credit card fraud.

The new subsection 1030(a)(5) to be created by the bill is designed to penalize those who intentionally alter, damage, or destroy certain computerized data belonging to another. The 'intentional' standard is the same as that employed in Section 2(a)(1) and 2(b)(1) of the bill. Like the new subsection 18 U.S.C. 1030(a)(3), this subsection will be aimed at 'outsiders,' i.e., those lacking authorization to access any Federal interest computer. It will penalize alteration, damage, or destruction in two circumstances. The first is those which cause a loss to the victim or victims totalling \$1,000 or more in any single year period. The Committee believes this threshold is ne-



cessary to prevent the bringing of felony-level charges against every individual who modifies another's computer data. Some modifications or alterations, while constituting 'damage' in a sense, do not warrant felony-level punishment, particularly when almost no effort or expense is required to restore the affected data to its original condition. The \$1,000 valuation has been reasonably calculated by the Committee to preclude felony punishment in those cases, while preserving the option of felony punishment in cases involving more serious alteration, damage, or destruction. In many instances where the requisite dollar amount cannot be shown, misdemeanor-level penalties will remain available against the offender under subsections 1030(a)(2) or 1030(a)(3).

The Department of Justice has suggested that the concept of 'loss' embodied in this subsection not be limited to the costs of \*2489 actual repairs. The Committee agrees and intends that other expenses accruing to the victim—such as lost computer time and the cost of reprogramming or restoring data to its original condition—be permitted to count toward the \$1,000 valuation. The Committee wishes to leave no doubt that it intends lost computer time to be covered by this subsection. Once again, the Committee recognizes the inherent value of using computer time or of occupying a portion of the time that a computer service is made available. Many commercial services obtain revenue by charging authorized subscribers for the amount of time they are using the service. An unauthorized user can therefore impose substantial costs on the service provider by tying up one channel of access—a channel that the provider might otherwise be leasing at a profit to an authorized subscriber. The Committee recognizes this danger, and intends subsection (a)(5) to cover cases where an offender, having obtained unauthorized access to the computer, prevents authorized use of such a computer by occupying an access channel or 'port' that is in demand by authorized subscribers. In the preceding discussion of subsection (a)(4), the Committee made clear that acts of trespass causing a loss of computer time should not be treated as acts of fraud for purposes of that subsection. However, it is clear that lost computer time can impose significant costs on providers of computer services. Where those costs total more than \$1,000 in any one-year period, the Committee believes prosecution should be available under this subsection.

Likewise, the Committee intends that certain network communications costs be permitted to count toward the \$1,000 valuation; a summary of a recent incident best illustrates this area. Often, a telecommunications firm (called the host company) will allow users from all over the country to access its computers by dialing a phone number that is local to the user. A second company (called a network company) will provide the service that connects the user, via phone lines, to the host company's computer, thus acting as a bridge between the two. The fee for the network company's service is often paid by the host company itself. In the incident under discussion, an unauthorized user programmed his computer to make repeated, automatic calls to the host company's computers in an effort to break into these computers. The effort to break in failed, but the user's automatic dialing mechanism made repeated use of the network company's communications service. In turn, the network company billed the host company for the time during which the unauthorized user had accessed its communications line. This is obviously unfair to the host company. Where billings to a host company for incidents such as this exceed \$1,000 in a one-year period, the Committee believes they should be subject to prosecution under this subsection.

Similarly, the Committee is concerned that authorized users of computer services might incur substantial costs as a result of relying on information contained in a database that has been tampered with. For example, an individual who invests in a stock, after having read a computerized market analysis that had been altered to make it appear the stock's potential had improved, has clearly \*2490 incurred a cost. The Committee intends that those costs also be permitted to count toward the \$1,000 valuation.

The second circumstance in which this subsection will penalize alteration, damage, or destruction is in connection with data relating to medical care and treatment. The Sloan-Kettering case discussed earlier in this report is but one example of computer crimes directed at altering medical treatment records. Where such conduct impairs or potentially impairs an individual's medical care, the Committee does not believe a showing of \$1,000 in financial losses is necessary. Tampering with computerized medical treatment records, especially given the



potentially life-threatening nature of such conduct, is serious enough to warrant punishment without a showing of pecuniary loss to the victim or victims. The Committee also wishes to make clear that convictions are attainable under this subsection without a showing that the victim was actually given an incorrect or harmful treatment, or otherwise suffered as a result of the changed medical record. That his examination, diagnosis, treatment, or care was potentially changed or impaired is sufficient to warrant prosecution under this subsection.

Two other important concerns have also been expressed to the Committee regarding the reach of the new subsection (a)(5). The first is that it might cover authorized 'repairs' to a computer system because 'alteration' of the data is part of the gravamen of the offense, and repairs presumably can involve altering data. It is not the Committee's intent to criminalize properly authorized repair activities. For example, this section does not prohibit employees of communications common carriers from engaging in activities that are necessary to the repair of the carrier's service. The Committee believes that the requirement in subsection (a)(5) that alterations occur after an unauthorized access is sufficient in itself to preclude its application to authorized repairs but wishes to leave no doubt that authorized repair activities are not covered by (a)(5).

The second concern is that (a)(5) might be construed as criminalizing the use in computer leasing services of automatic termination devices or so-called 'time bombs'. Frequently, a provider of computer services will build into his program a mechanism that automatically terminates the service if a user fails to pay his bill for the service on time. Concerns have been expressed that the provider might be considered liable under (a)(5) for having 'prevented authorized use' of the service. That is not the Committee's intent. Having failed to pay his bill for the Committee service, the delinquent user is no longer an 'authorized user' of the service, and termination of his access to the service is not an offense under this subsection.

The new subsection 1030(a)(6) to be created by the bill is a misdemeanor offense aimed at penalizing conduct associated with 'pirate bulletin boards,' where passwords are displayed that permit unauthorized access to others' computers. It will authorize prosecution of those who, knowingly and with intent to defraud, traffic in such computer passwords. If those elements are present—and if the password in question would enable unauthorized access to a Federal Government computer, or if the trafficking affects interstate or foreign commerce—this subsection may be invoked. The concept of \*2491 'traffic' means to transfer, or otherwise dispose of, to another, or to obtain control of with intent to transfer or dispose of such passwords; the concept was borrowed from 18 U.S.C. 1029 relating to credit card offenses. The Committee also wishes to make clear that 'password', as used in this subsection, does not mean only a single word that enables one to access a computer. The Committee recognizes that a 'password' may actually be comprised of a set of instructions or directions for gaining access to a computer and intends that the word 'password' be construed broadly enough to encompass both single words and longer more detailed explanations on how to access others' computers.

Section 2(c) eliminates the specific conspiracy offense in the present law. The Committee intends that such conduct be governed by the general conspiracy offense in 18 U.S.C. 371.

Section 2(f) conforms the 'fine' provisions of 18 U.S.C. 1030 and this bill with the general fine provisions of the Criminal Fine Enforcement Act of 1984. It also contains the penalty provisions for the two new felony provisions (5 years first offense, 10 years second offense) and one new misdemeanor/felony provision (one year first offense, 10 years second offense).

Section (2)(g) establishes definitions for a 'Federal interest computer,' 'State,' 'financial institution,' 'financial record,' the term 'exceeds authorized access,' and the term 'department of the United States,' all of which are self-explanatory. The only committee note is that obtaining information as encompassed in the definition for 'exceeds authorized access' would include observing information as we discussed under Section 2(a)(2) *supra*.

Section 2(h) conforms the exception for proper law enforcement and intelligence activity in the computer crime bill with the credit card legislation in 18 U.S.C. 1029(f).

Finally, the Committee wishes to make two general observations that apply to each of the computer crime offenses amended or created by S. 2281.

First, the Committee recognizes the necessity that computerized information be considered 'property' for purposes of Federal criminal law. To date, computer users for providers of computer services have had to wrestle with a criminal justice system that in many respects is ill-equipped to handle their needs. Computer technology simply does not fit some of the older, more traditional legal approaches to theft or abuse of property. For example, computer data may be 'stolen' in the sense that it is copied by an unauthorized user, even though the original data has not been removed or altered in any way. As long ago as 1983, the Department of Justice stated that:

Any enforcement action in response to criminal conduct indirectly or directly related to computers must rely upon a statutory restriction dealing with some other offense. This requires the law enforcement officer, initially the agent, and then the prosecutor, to attempt to create a 'theory of prosecution' that somehow fits what may be the square peg of computer fraud into the round hole of \*2492 theft, embezzlement or even the illegal conversion of trade secrets.<sup>13</sup>

These enforcement problems can largely be overcome by recognizing computerized information as property. The Congress began that recognition by enacting the Computer Fraud and Abuse Act of 1984. The Committee intends S. 2281 to affirm the government's recognition of computerized information as property.

Secondly, the Committee wishes to make clear its intent to distinguish between conduct that is completely inadvertent and conduct that is initially inadvertent but later becomes an intentional crime. It has been suggested that this is a difficult line to draw in the area of computer technology because of the possibility of mistakenly accessing another's computer files. Nevertheless, the Committee would expect one whose access to another's computer files or data was truly mistaken to withdraw immediately from such access. If he does not and instead deliberately maintains unauthorized access after a non-intentional initial contact, then the Committee believes prosecution is warranted. The individual's intent may have been formed after his initial, inadvertent access. But his is an intentional crime nonetheless, and the Committee does not wish to preclude prosecution in such instances.

#### IV. AGENCY VIEWS

In its testimony on April 16, 1986, the Department of Justice supported S. 2281, although it recommended several amendments to the bill.<sup>14</sup> The Committee adopted some of those recommendations, including an amendment clarifying the degree to which the offense in subsection 1030(a)(3) must affect the operation of the Government computer in question. Many of the Department's recommendations were incorporated into the Committee's report on S. 2281.

#### V. CONGRESSIONAL BUDGET OFFICE STATEMENT

U.S. CONGRESS,  
CONGRESSIONAL BUDGET OFFICE,  
*Washington, DC, June 25, 1986.*

Hon. STROM THURMOND,  
*Chairman, Committee on the Judiciary, U.S. Senate, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has reviewed S. 2281, the Computer Fraud and Abuse Act of 1986, as ordered reported by the Senate Committee on the Judiciary, June 12, 1986. We estimate that no significant cost to the Federal Government, and no cost to State or local governments would result from enactment of this bill.

S. 2281 makes a number of amendments to Section 1030 of Title 18 of the United States Code, dealing with

computer fraud and related activity. These amendments include several changes in the standards determining violations of the law. The bill extends the \*2493 existing Federal privacy protection of computerized financial information to cover all such records of financial institutions, as defined in the bill, and clarifies the prohibition against unauthorized access of computers used by the U.S. government. S. 2281 also creates three new offenses involving theft in the form of unauthorized computer access with the intent to defraud, malicious damage through unauthorized computer access, and trafficking in computer passwords with the intent to defraud. The provisions governing fines for new and existing offenses would be made to conform with the Criminal Fine Enforcement Act of 1984.

Based on information from the Department of Justice, we expect that S. 2281 would provide a more specific statute on which to base the investigation and prosecution of these activities, which the Department is currently undertaking under other authority. Enactment of the bill is not expected to result in a significant change in the government's law enforcement practices or expenditures.

If you wish further details on this estimate, we will be pleased to provide them.

With best wishes,  
Sincerely,

RUDOLPH G. PENNER.

#### VI. REGULATORY IMPACT STATEMENT

Pursuant to paragraph 11(b), rule XXVI, of the Standing Rules of the Senate, the Committee has concluded that the bill will have no direct regulatory impact. The bill encourages, but does not require, the agencies and departments of the Federal Government to develop clear rules and sanctions regulating the use of Government computers by employees and other authorized individuals. The bill also encourages other owners and users of Federal interest computers to establish clear statements of the scope of authority for those who use the Federal interest computers.

\* \* \* \* \*

#### VIII. ADDITIONAL VIEWS OF MESSRS. MATHIAS AND LEAHY

We are pleased to join with our colleagues on the Judiciary Committee in reporting S. 2281, the Computer Fraud and Abuse Act of 1986. The authors of the legislation have effectively carried out a delicate and complex task. The result is a bill that offers an appropriate Federal response to the real and growing problem of computer crime.

The committee's report on S. 2281 thoroughly describes the scope of that problem, and the details of that response. As the report notes, this bill builds upon the computer crime legislation enacted in the closing days of the 98th Congress. We wish to emphasize that S. 2281 not only refines and extends the computer crime provisions of Public Law 98-473, it also refocuses that legislation on its principal objectives, and minimizes the likelihood that it will be misused to cut back on the American public's right to know about the activities of its government.

\*2494 As enacted in 1984, the provision now codified as section 1030(a)(3) of title 18 makes it a crime to 'knowingly use . . . or disclose information in [any] computer . . . operated for or on behalf of the Government of the United States,' when the defendant gains access to the computer without authorization or his conduct exceeds the scope of his authorization. By its literal terms, this provision sweeps in all computerized government information, including documents that must, under the Freedom of Information Act, be disclosed to any member of the public upon proper request. Section 1030(a)(3) also glosses over the reality that the existence or exact scope of a government employee's authority to access a particular computerized data base is not always free

from doubt. Under these circumstances, any employee asked to release data that must be disclosed under the FOIA would be understandably reluctant to do so unless assured of the precise contours of his authorization to access it. An incorrect assertion of authorization could expose the employee to prosecution and imprisonment. Any prudent employee would resolve doubts against disclosure, a conclusion directly contrary to the principles of open government underlying the FOIA.

Motivated by these concerns arising from provisions of the House-passed computer crime bill, the Senate, on the next-to-last day of the 98th Congress, unanimously approved our amendment to the bill which narrowed the sweeping provisions of the disclosure offense under section 1030(a)(3). Unfortunately, in the rush toward adjournment, the House never acted on the Senate amendment to this bill. Instead, the free-standing computer crime legislation was overtaken by a continuing appropriations resolution, to which had been appended hundreds of pages of crime legislation, including portions of the unamended House computer crime bill. Thus, in a particularly graphic lesson in the shortcomings of legislation by rider, section 1030(a)(3) was signed into law, despite the Senate's unanimous view that its scope was too broad.

The bill we now report, unlike its predecessor, has had the benefit of nearly 2 years of careful scrutiny and study by the Subcommittee on Criminal Law. Among the many improvements that it would make is a complete revision of section 1030(a)(3). The revised provision includes three salutary features that minimize the possibility that this computer crime legislation could be misused to weaken the Freedom of Information Act, or to impose unnecessary obstacles to the public's right to know about government activities.

First, the mental state required to establish a violation of revised section 1030(a)(3) is increased from 'knowingly' to 'intentionally.' As the committee report points out, the 'intentional' standard precludes criminal liability for inadvertent acts of unauthorized access. Instead, it is 'designed to focus Federal criminal prosecutions on those who evince a clear intent to enter, without proper authorization, computer files or data belonging to another.'

Second, S. 2281 would eliminate coverage for authorized access that aims at 'purposes to which such authorization does not extend.' This removes from the sweep of the statute one of the murkier grounds of liability, under which a Federal employee's access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances.\*2495 that might be held to exceed his authorization. As the committee report points out, administrative sanctions should ordinarily be adequate to deal with real abuses of authorized access to Federal computers (assuming, of course, that no other provision of section 1030 is violated). Like the heightened scienter requirement, this change serves to minimize the likelihood that a Federal employee, uncertain about the scope of his authority, would face a Hobson's choice between the disclosure mandates of FOIA and the criminal sanctions of title 18.

Finally, revised section 1030(a)(3) would not apply to access by a Federal employee of computers of that employee's own agency. This exclusion recognizes the reality that computer access rules for employees within a single agency are rarely as clear as rules governing access by outsiders to that agency's computers. Revised section 1030(a)(3) would provide prosecutors a clear, workable rule, regardless of the intricacies of a particular agency's computer access policies: absent a fraudulent motive, an employee could not be prosecuted for simple 'trespass' into one of his agency's own computers.

Like any bright-line rule, this one does not conform perfectly to the behavior it addresses. To treat employees of other agencies as 'outsiders' for the purposes of this statute may, in an exceptional instance, work some hardship. The committee report notes that the revised subsection may, on rare occasions, prove underinclusive; as well, it may be overinclusive in unusual cases. The fact is that many Federal agency data bases are separated from those of sister agencies not by well-defined walls, but by permeable membranes. Information sharing may become computer sharing without formal protocols of authorization. Access by one who appears to be an 'outsider' to the agency may be not only excusable, but helpful to the agency's mission.

But certainly this imprecision can be accommodated. Just as other criminal sanctions may well be at hand in cases that fall through the net of the revised subsection (a)(3), so administrative sanctions—and, of course, the discretion not to prosecute—will remain available for those cases of interdepartmental unauthorized access that do not justify prosecution.

S. 2281's revisions to section 1030(a)(3) do not track the approach adopted by the Senate in 1984, and embodied in our bill in this Congress, S. 610, for correcting the course set by the 1984 computer crime legislation. Both the 1984 Senate amendment, and S. 610, focused on the disclosure aspect of the offense created by section 1030(a)(3), and sought to exclude from the offense information whose disclosure ought not to be discouraged. Because the revised subsection is a simple trespass offense, rather than one requiring disclosure or some other act beyond access to the data, our earlier approach to the problem is now less apposite. We think the balance struck by S. 2281 on this issue is reasonable. It largely ameliorates our concern about the effect of section 1030(a)(3) on the free flow of government information to the American people. It goes far toward restoring the incentive for Federal employees to comply voluntarily with the Freedom of Information Act in their dealings with requests<sup>2496</sup> for computerized government information. At the same time, it gives the Government an adequate prosecutorial tool for deterring and punishing unauthorized access to sensitive Government information by those who have no colorable claim of a right to obtain it outside proper channels.

In this and other aspects, S. 2281 constitutes a real improvement on existing computer crime law. The Subcommittee on Criminal Law, under Senator Laxalt's leadership, and its House counterpart, the Subcommittee on Crime, have crafted well-considered and constructive legislation, and we are pleased to support it.

1 Bureau of Justice Statistics, *Report on Electronic Funds Transfer Fraud*, March 1985, NCJ-96666.

2 *Report on Computer Crime*; Task Force on Computer Crime, Section of Criminal Justice, American Bar Association; June 1984)

3 Ibid., pp. 16–18, Table 12.

4 Ibid., p. 38.

5 Ibid., pp. 36–40.

6 Ibid., p. 44.

7 Ibid., p. 23, Table 17.

8 Ibid., p. 11, Table 8.

9 Ibid., p. 23, Table 17.

9a. 98 S.Ct. 2864, 57 L.Ed.2d 854.

10 Statement of Victoria Toensing, Deputy Assistant Attorney General, Criminal Division; before the Senate Judiciary Committee, April 16, 1986.

11 Ibid.

12 Ibid.

13 Statement by John C. Keeney, Deputy Assistant Attorney General, Criminal Division; before the Senate Subcommittee on Oversight of Government Management, Committee on Governmental Affairs; October 26, 1983.

14 See, Statement of Victoria Toensing, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, before the Senate Judiciary Committee; April 16, 1986.

S. Rep. No. 432, 99TH Cong., 2ND Sess. 1986, 1986 U.S.C.C.A.N. 2479, 1986 WL 31918, S. REP. 99-432 (Leg.Hist.)

END OF DOCUMENT

## UNITED STATES

**ADDENDUM TO  
DEFENSE MOTION TO  
COMPEL DISCOVERY #2**

v.

**MANNING, Bradley E., PFC**  
**U.S. Army, xxx-xx-██████████**  
 Headquarters and Headquarters Company, U.S.  
 Army Garrison, Joint Base Myer-Henderson Hall,  
 Fort Myer, VA 22211

7 June 2012

1. On 7 June 2012, the Court heard testimony from the following Department of State witnesses:

- (a) Ms. Marguerite Coffey;
- (b) Ms. Rena Bitter; and
- (c) Ms. Catherine Brown.

2. Each witness testified about their personal knowledge concerning whether the following documents existed with respect to the following within the Department of State:

- (a) The Chiefs of Mission review of the released cables at affected posts discussing their initial assessment, as well as their opinion regarding the overall effect that the WikiLeaks release could have on relations within their host country, if any;
- (b) The WikiLeaks Working Group composed of senior officials throughout the Department that was created to review potential risks to individuals from the release of cables by WikiLeaks, if any;
- (c) The "Mitigation Team" created by the Department of State to address the policy, legal, security, counterintelligence, and information assurance issues presented by the release of the documents to WikiLeaks, if any;
- (d) The Persons at Risk Working Group created by the Department of State to identify any individuals that may be placed at risk due to the publication of the diplomatic cables and to address any measures that may be needed; AND

(e) The Department's reporting to Congress concerning any effect caused by the WikiLeaks' disclosure and the steps undertaken to mitigate them, if any. The Department convened two separate briefings for members of both the House of Representatives and the Senate in December of 2010. The Department also appeared twice before the House Permanent Select Committee on Intelligence on 7 and 9 December 2010.

3. The above listed witnesses' testimony confirmed the existence of Defense requested records. The testimony also disclosed the following additional information:

(a) The Chiefs of Mission produced written assessments of the leaked cables based upon their independent review. These written submissions were then used to formulate a portion of the draft damage assessment completed in August of 2011;

(b) The WikiLeaks Working Group created a written Situation Reports approximately twice a week during the groups time period of operation roughly from 28 November 2010 until 17 December 2010.

(c) The Department of State Mitigation Team had written minutes of its meetings and written agendas for it work. Part of the Mitigation Team's efforts concentrated on counterterrorism concerns;

(d) The Persons at Risk Group created and Information Memorandum for the Secretary of State and a matrix to track identified individuals. The Group also put out formal guidance to all embassies concerning the Department of States' efforts and authorized actions for any identified person at risk; AND

(e) The Director of the Office of Counterintelligence within the Department of State had been collecting information regarding any possible impact from the disclosure of diplomatic cables. The collection of this information was intended to possibly be used to update the August 2011 draft damage assessment should the Department consider this a worthwhile endeavor.

(f) The Department of State's reporting to Congress. The Department likely produced a prepared written statement for the testimony on 7 and 9 December 2010 as it had done for Ambassador Patrick Kennedy's testimony on 11 March 2011.

4. The Government has a due diligence duty to search for evidence that is favorable to the defense and material to guilt or punishment. *Brady v. Maryland*, 373 U.S. 83, 87 (1963); R.C.M. 701(a)(6). The trial counsel's due diligence duty applies to: "(1) the files of law enforcement authorities that have participated in the investigation of the subject matter of the charged offense; (2) investigative files in a related case maintained by an entity closely aligned with the prosecution; and (3) other files, as designated in a defense discovery request, that involved a specified type of information within a specified entity." *United States v. Williams*, 50 M.J. 436, 441 (C.A.A.F. 1999) (internal quotations and citations omitted).

5. "For relevant files known to be under the control of another governmental entity, Trial Counsel must make the fact known to the Defense and engage in good faith efforts to obtain the material." Appellate Exhibit XXXVI at 8, para. 3. The Defense has requested the above specific information from within the Department of State.



6. There may, of course, be other files at the Department of State of which the Defense is unaware. The trial counsel bears an obligation to search these files, *in addition to those specified above*, pursuant to the second prong of *Williams*.

7. The Defense maintains that all of the above information is discoverable under R.C.M. 701(a)(6) and R.C.M. 701(a)(2).

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

**Lind, Denise R COL USARMY (US)**

---

**From:** David Coombs [coombs@armycourtartialdefense.com]  
**Sent:** Thursday, June 07, 2012 9:46 PM  
**To:** Lind, Denise R COL USARMY (US); Williams, Patricia A CIV (US); Jefferson, Dashawn MSG USARMY (US)  
**Cc:** Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US); Fein, Ashden MAJ USARMY (US); Overgaard, Angel M CPT USARMY (US); 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; Whyte, Jeffrey H CPT USARMY (US); Alexander.VonElten@jfhqncr.northcom.mil  
**Subject:** Court's Questions  
**Attachments:** Responses to Court questions.docx; United States v Jones.docx

Ma'am,

The Court had several questions for the Defense during today's motions argument. In particular, the Court asked the Defense the following questions:

- 1) What is the Court's authority to dismiss the 1030 offenses?
- 2) How does the Defense interpret the passage quoted by the Court from the legislative history of section 1030?
- 3) Does the elements test require a Court to look at the elements as charged or simply the statutory elements?

The Defense has provided further responses in the Attachment (and has provided a case in support of the Court's authority to dismiss the 1030 offenses).

Best,

David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906

Toll Free: 1-800-588-4156

Local: (508) 689-4616

Fax: (508) 689-9282  
[coombs@armycourtartialdefense.com](mailto:coombs@armycourtartialdefense.com) <<mailto:coombs@armycourtartialdefense.com>>

[www.armycourtartialdefense.com](http://www.armycourtartialdefense.com) <<http://www.armycourtartialdefense.com/>>

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

## **1. Court's Authority to Dismiss for Failure to State an Offense**

The Court asked the Defense today what authority the Court had to dismiss an offense if the Defense concedes all the facts alleged by the Government and the conduct still does not amount to a cognizable offense. The Defense indicated that you had inherent authority to do so. Upon further research, the Defense submits that your authority also derives from R.C.M. 907(b)(1)(B). For ease of reference, the relevant sections of R.C.M. 907 are as follows:

### **Rule 907. Motions to dismiss**

- (a) *In general.* A motion to dismiss is a request to terminate further proceedings as to one or more charges and specifications on grounds capable of resolution without trial of the general issue of guilt.
- (b) *Grounds for dismissal.* Grounds for dismissal include the following –
  - (1) *Nonwaivable grounds.* A charge or specification shall be dismissed at any stage of the proceedings if: ...
    - (B) The specification fails to state an offense.

When you look at the Drafter's Comments, you see that R.C.M. 907(b)(1) is based upon Federal Rules of Criminal Procedure 12(b)(2) ("(2) Motions That May Be Made Before Trial. A party may raise by pretrial motion any defense, objection, or request that the court can determine without a trial of the general issue.") and 34 ("Arresting judgment"). Thus, it is clear that the Drafter's intended to parallel the power of a federal court to dismiss for failure to state an offense. In fact, if you look at Federal Rule of Criminal Procedure 12 (below), you see that R.C.M. 907(b)(1)(B) is actually more specific than its federal counterpart in terms of the power of a military judge to dismiss a specification for failure to state an offense.

### **Rule 12**

(a) **PLEADINGS.** The pleadings in a criminal proceeding are the indictment, the information, and the pleas of not guilty, guilty, and nolo contendere.

(b) **PRETRIAL MOTIONS.**

(1) *In General.* Rule 47 applies to a pretrial motion.

(2) *Motions That May Be Made Before Trial.* A party may raise by pretrial motion any defense, objection, or request that the court can determine without a trial of the general issue.

(3) *Motions That Must Be Made Before Trial.* The following must be raised before trial:

(A) a motion alleging a defect in instituting the prosecution;

(B) a motion alleging a defect in the indictment or information—but at any time while the case is pending, the court may hear a claim that the indictment or information fails to invoke the court’s jurisdiction or to state an offense;

(C) a motion to suppress evidence;

(D) a Rule 14 motion to sever charges or defendants; and

(E) a Rule 16 motion for discovery.

The key, under both federal and military law, is whether the issue can be is “capable of resolution without trial of the general issue of guilt.” In this case, the issue at hand – whether PFC Manning exceeded authorized access within the meaning of section 1030 – clearly is capable of resolution without trial based on the Defense’s concessions for the purposes of this motion only. If the Court finds that “exceeds authorized access” must be interpreted as the Defense suggests, the Court must accordingly dismiss the specification.

The Defense directs the Court’s attention to *United States v. Jones*, 60 M.J. 917 (N-M.C.C.A. 2005) for a case on point. There, the accused – a midshipman – was originally charged with fraternization under certain Navy Regulations. The Court granted a defense motion to dismiss for failure to state an offense “because midshipmen do not qualify as either officers or enlisted persons for purposes of fraternization” under the charged regulation. *Id.* at 918. A separate Convening Authority later re-preferred charges under a different regulation that did apply to midshipmen. The key is that the trial court did not need to wait until the Government failed to prove that the accused either an officer or enlisted and then dismiss the case under R.C.M. 917.

Accordingly, the Defense submits that this Court has authority under R.C.M. 907(b)(1)(B) to dismiss the charged offenses.

## 2) Legislative History of 1030

The Court asked the Defense about a certain passage that it quoted with respect to Section 1030’s legislative history. The legislative history of Section 1030, including the history behind the 1996 amendments to Section 1030(a)(1), fully supports the Defense’s interpretation of the phrase “exceeds authorized access.” The Senate Report accompanying the 1996 Amendments explained the interplay between the espionage laws and Section 1030(a)(1):

Although there is considerable overlap between 18 U.S.C. [Section] 793(c) and [S]ection 1030(a)(1), as amended by the NII Protection Act, the two statutes would not reach exactly the same conduct. Section 1030(a)(1) would target those persons who deliberately *break into a computer* to obtain properly classified Government secrets then try to peddle those secrets to others, including foreign governments. In other words, unlike existing espionage laws prohibiting the theft and peddling of Government secrets to foreign agents, [S]ection 1030(a)(1) would require proof that the individual knowingly used a computer without authority, or in excess of authority, for the purpose of obtaining classified information. In this

sense then, it is the use of the computer which is being proscribed, not the unauthorized possession of, access to, or control over the classified information itself.

S. Rep. No. 104-357 (1996) (emphasis supplied). The term “use” in the last sentence of the above-quoted language must be read in the context of the *entire* passage. The passage makes clear that the phrase “use of the computer” in the last sentence does not simply refer to any general computer use. The sentence before it explains that Section 1030(a)(1) punishes one who knowingly “used a computer *without authority, or in excess of authority*, for the purpose of obtaining classified information.” *Id.* (emphasis supplied). Therefore, the term “use” in the phrase “it is the use of the computer which is being proscribed,” when properly read in context of the entire passage, refers only to use without authority or use in excess of authority.

At bottom, the final two sentences of the above-quoted Senate Report are merely offered to refine the passage’s clear statement of whom Section 1030(a)(1) targets: “those persons who deliberately *break into a computer* to obtain properly classified Government secrets[.]” *Id.* (emphasis supplied). General use of a computer does not require in all cases a person to “break into” the computer; thus, the term “use” in the last sentence of this passage cannot mean general use of a computer. Rather, it means use that involves breaking into the computer (i.e. accessing a computer without authorization or in excess of authority) by bypassing technical restrictions on access. Just as a person who steals jewelry from another’s home after being invited in has not broken into the home merely because he commits a crime therein, a person who is authorized to access the computer and information has not broken into that computer or any part of it merely because he later uses that information for improper purposes. Holding that Section 1030(a)(1) punishes someone who uses a computer for certain purposes without requiring that the user first break into that computer by violating technical restrictions on access would be akin to holding that burglary punishes someone who commits a crime inside another’s home without requiring that the person first break into the home. Because Section 1030(a)(1) punishes one who breaks into a computer, the only “use” that it can proscribe is use without authority or in excess of authority; in either case, bypassing technical restrictions is required to break into the computer.

Finally, none of the cases cited by the Government or any other case of which the Defense is aware adopting the expansive interpretation of the term “exceeds authorized access” have relied on (or even mentioned) the term “use” in the third sentence of the above-quoted Senate Report. In fact, to the Defense’s knowledge, no case has ever even cited this portion of the legislative history.

### **3) Elements Test for LIO Determination**

The Court also asked the Defense for authority that the elements test required looked at the elements *as charged*, rather than looking simply at the statutory elements. It is well-settled that the comparison of the statutory elements as charged in the specification is permitted in an elements test analysis. In addition to *United States v. Arriaga*, 70 M.J. 51, 54-55 (C.A.A.F. 2011), the Court of Appeals for the Armed Forces’ earlier decision in *United States v. Alston*, 69 M.J. 214 (C.A.A.F. 2010), also clearly makes this point. In *Alston*, the Court determined that aggravated sexual assault under Article 120(c)(1)(B) was a LIO of rape by force under Article 120(a)(1). 69 M.J. at 216. In reaching this conclusion, the Court was required to compare the

elements of the offenses *as charged in the specification* because a comparison of the statutory elements in the abstract would not have led to the conclusion that aggravated sexual assault was a LIO of rape by force. *See id.* Article 120(t)(5) provides three different methods by which the force element of rape by force can be established, and only one of those methods necessarily included the “offensive touching” necessary for the “causing bodily harm” element of the aggravated sexual assault offense. *Id.* In conducting its elements test analysis, the *Alston* Court expressly relied on how the elements were charged in the specification:

The second element of aggravated sexual assault – “causing bodily harm” under Article 120(c)(1)(B) – means “any offensive touching of another, however slight.” Article 120(t)(8). The parallel element in the offense of rape *as charged in the present case* – using “force” under Article 120(a)(1) – means “action to compel submission of another or to overcome or prevent another’s resistance by . . . physical violence, strength, power, or restraint applied to another person, sufficient that the other person could not avoid or escape the sexual conduct.” Article 120(t)(5)(C).

\* \* \*

We note that the definitions of force in Article 120(t)(5)(A) and Article 120(t)(5)(B), which do not require an offensive touching, *are not at issue in the present case*.

*Id.* (emphases supplied). Thus, by examining the elements as charged (and by ignoring statutory definitions not at issue in the case), the *Alston* Court established that consideration of the elements of the offenses as charged in the specification is permissible under the elements test analysis. If comparison of the elements as charged in the specification was not permitted, the *Alston* Court would have been unable to conclude that aggravated sexual assault under Article 120(c)(1)(B) was a LIO of rape by force under Article 120(a)(1). Indeed, the *Arriaga* Court relied on the *Alston* Court’s analysis in reaching the same conclusion a year later: “[U]nder *United States v. Alston*, 69 M.J. 214 (C.A.A.F. 2010), comparison of the statutory elements *as charged in the specification* is allowed[.]” *Arriaga*, 70 M.J. at 54 (emphasis supplied); *see also id.* at 55 (“Regardless of whether one looks strictly to the statutory elements or to the *elements as charged*, housebreaking is a [LIO] of burglary . . . . [T]he offense *as charged in this case* clearly alleges the elements of both offenses.” (emphases supplied)); *id.* (“The offense *as charged* included all of the elements of housebreaking and all of those elements are also elements of burglary. Housebreaking is therefore a lesser included offense of burglary.” (emphasis supplied)).

In the wake of *Alston* and *Arriaga*, two very recent decisions from the CAAF, it is clear that comparison of the elements as charged in the specification is permitted in an elements test analysis. *See United States v. Nealy*, 71 M.J. 73, 79 & n.1 (C.A.A.F. 2012) (Baker, C.J., concurring in the result) (explaining that, under *Arriaga*, the specification itself may provide notice to an accused of the LIOs of the charged offense(s)).

60 M.J. 917  
(Cite as: 60 M.J. 917)

## H

U.S. Navy-Marine Corps Court of Criminal Appeals.  
UNITED STATES

v.

Ronald D. JONES, Staff Sergeant (E-6), U.S. Marine Corps.

NMCCA 200401276.  
Decided 16 Feb. 2005.

**Background:** Government appealed military judge's ruling in special court-martial dismissing charged offenses without prejudice for improper referral.

**Holding:** The United States Navy-Marine Corps Court of Criminal Appeals, Wagner, J., held that re-referral of offenses to second special court-martial by a different convening authority was not improper on ground that re-referral was more onerous, and thus court-martial rule required that reasons for the withdrawal and re-referral of charges be included in the record.

Appeal granted.

### West Headnotes

#### [1] Military Justice 258A ↪ 967.1

258A Military Justice

258AIV Pretrial Proceedings

258AIV(B) Charges and Specifications and Action Thereon

258Ak967 Referral for Trial

258Ak967.1 k. In General. Most Cited Cases

A command other than the one to which the accused is attached may refer charges against the accused to a court-martial. R.C.M. 601(b).

#### [2] Military Justice 258A ↪ 968

258A Military Justice

258AIV Pretrial Proceedings

258AIV(B) Charges and Specifications and Action Thereon

258Ak967 Referral for Trial

258Ak968 k. Withdrawal and Re-Referral. Most Cited Cases

Re-referral of offenses to second special court-martial by a different convening authority was not improper on ground that re-referral was more onerous, and thus court-martial rule required that reasons for the withdrawal and re-referral of charges be included in the record; re-referral was not more onerous than original referral, and reasons for dismissal were a matter of record at second court-martial. R.C.M. 604(b).

\*917 LtCol JosephR. Perlak, USMC, Appellate Defense Counsel.

Lt Colin Kisor, JAGC, USNR, Appellate Defense Counsel.

CDR CharlesN. Purnell, JAGC, USN, Appellate Government Counsel.

Lt Kathleen Helmann, JAGC, USNR, Appellate Government Counsel.

Before CARVER, Senior Judge, WAGNER, and REDCLIFFE, Appellate Military Judges.

WAGNER, Judge:

This case is before us on Government appeal of the military judge's ruling to dismiss without prejudice the charged offenses for improper referral of charges. The appeal is properly brought before this court under Article 62, Uniform Code of Military Justice, 10 U.S.C. § 862. After a thorough review of the entire record of trial and the briefs submitted by the Government and the appellee, we find that the military judge erred in dismissing the charged offenses on the basis of improper referral.

### Facts

The appellee, a Marine staff sergeant, was assigned as a senior enlisted instructor for the midshipmen at the United States Naval Academy. As a



60 M.J. 917  
(Cite as: 60 M.J. 917)

result of an investigation into an alleged improper relationship between the appellee and a female midshipman during the period of June 2001 to May 2002, the appellee was relieved from his duties at the Naval Academy in August of 2002 and reassigned to his administrative unit, Marine Barracks, Washington, D.C. Shortly thereafter, he executed permanent change of station orders to Headquarters and Service Battalion (H & SBN), Marine Corps Base (MCB), Quantico, VA. A report of investigation was forwarded to H & SBN by the Naval Academy.

Following review of the report of investigation, the Commanding Officer, H & SBN, the appellee's immediate commander and a special court-martial convening authority (SPCMCA), determined that the adverse administrative actions taken were sufficient and did not initiate any disciplinary action. Thereafter, the Commanding General, MCB, Quantico, his next senior commander and a general court-martial convening authority (GCMCA), assumed authority over the disposition of the report of investigation and, on 26 \*918 March 2003, referred charges against the appellee to a special court-martial (SPCM) convened by him. The charges included fraternization in violation of Article 1165, U.S. Navy Regulations (1990), assault, drunk and disorderly, indecent language, and solicitation to commit an offense.

At a post-arraignment Article 39(a) session on 23 June 2003, the military judge granted a defense motion to dismiss the fraternization offenses for failure to state an offense because midshipmen do not qualify as either officers or enlisted persons for purposes of fraternization under U.S. Navy Regulations. There is no record of these proceedings, nor is there any written documentation that the offenses were ever withdrawn and dismissed or whether they were dismissed with or without prejudice.

Following a routine change of command at MCB Quantico, Commander, MCB, Quantico became the successor in command and was also designated a GCMCA. The staff judge advocate (SJA) for the Superintendent of the Naval Academy began an aggressive campaign to convince the Commander, MCB, Quantico, to re-refer the charges to another court-martial, including charges of forcible sodomy and indecent assault based on the appellee's superior/subordinate status as a senior enlisted advisor vis-à-vis the female midshipman. During the course of

this campaign, the SJA for the Superintendent not only spoke several times with the legal staff for the Commander, MCB, Quantico, he took the highly unusual step of speaking directly to the Commander himself. The SJA for the Superintendent expressed his belief that the Commander, MCB, Quantico, had not been adequately briefed on the facts of the case by his own SJA, that the Marine commanders did not understand the relationship of a midshipman to a senior enlisted advisor, and that the Marine Corps in general had "dropped the ball" in this case. Record at 256.

The Commander, MCB, Quantico, directed additional investigation into the original incidents, including a re-interview of the midshipman. After a review of all the evidence, the Commander, MCB, Quantico, concurred with the recommendation of his SJA not to refer charges to another court-martial. In particular, the Commander, MCB, Quantico, found no evidence that the alleged sexual activity was not consensual and no basis to charge the appellee with either forcible sodomy or indecent assault. The Commander, MCB, Quantico, told the SJA for the Superintendent that he would make the appellee available for trial in the event the Superintendent, a GCMCA, convened a court-martial and referred charges against the appellee.

On 12 March 2004, the Superintendent of the Naval Academy did, in fact, convene a special court-martial and refer charges involving sexual harassment, fraternization in violation of Chief of Naval Operations Instruction 5370.2B (27 May 99), dereliction of duty, forcible sodomy, indecent assault, and drunk and disorderly conduct. These charges arose from the same incidents that occurred when the appellee was assigned to the Naval Academy.

At a post-arraignment Article 39(a) session on 29 June 2004, during his second court-martial, the appellee moved for dismissal of all charges and specifications on the basis of unlawful command influence, lack of subject matter jurisdiction, and improper referral. Extensive testimony, evidence, and argument were presented regarding the propriety of the actions of the SJA for the Superintendent in his attempts to influence the Commander, MCB, Quantico, to refer charges anew. With respect to the disposition of the earlier charges, the trial counsel from the first court-martial testified that he recalled discussing options with the convening authority's military justice

60 M.J. 917  
(Cite as: 60 M.J. 917)

officer and then withdrawing and dismissing the offenses on the record.

The intent of the convening authority to withdraw and dismiss the original charges is further supported by Appellate Exhibit VII, a memorandum dated 8 October 2003 to Commander, MCB, Quantico, from his SJA, recommending a decision terminating disciplinary action against the appellee. That memorandum indicates that the remaining charges were withdrawn and re-drafted at some unspecified time and that the SJA for the Superintendent of the Naval Academy had requested that the re-drafted charges be re-preferred. The Commander, MCB, Quantico,\*919 terminated further action on those charges by approving his SJA's recommendation. The military judge, however, in a written order dated 26 August 2004, dismissed without prejudice the offenses on the sole basis of improper referral. Appellate Exhibit XVII.

The Government now appeals the order of the trial court dismissing the offenses and asks this court to reverse the trial judge's decision. We are limited by Article 62, UCMJ, 10 U.S.C. § 862, to review only those issues raised by the government on appeal.

#### Issues

The Government claims two bases for error in the military judge's dismissal of the charges. First, the Government asserts that the military judge erred by finding that an obvious disagreement existed between the two convening authorities as to the disposition of the case that required resolution by a superior competent authority. Second, the Government contends that the military judge erred by finding that the second referral was more onerous to the appellee than the first and, therefore, that the reasons for the prior withdrawal and subsequent re-referral must be provided in the record of the subsequent court-martial.

#### Standard of Review

The standard of review in this case is abuse of discretion. United States v. Gore, 60 M.J. 178, 187 (C.A.A.F.2004); United States v. Hatfield, 43 M.J. 662, 664 (N.M.Cr.Crim.App.1995), *rev'd on other grounds*, 44 M.J. 22 (C.A.A.F.1996). Review by this court is limited to matters of law and we are required to defer to the findings of fact of the trial judge so long as they are "fairly supported by the record'...." Gore, 60 M.J. at 185 (quoting Marshall v. Lonberger, 459 U.S. 422, 103 S.Ct. 843, 74 L.Ed.2d 646 (1983)). The

Government, as appellant, carries the burden of persuasion that the military judge abused his discretion. United States v. Houser, 36 M.J. 392, 397 (C.M.A.1993); Hatfield, 43 M.J. at 664. This court may not substitute its judgment for that of the trial judge. United States v. Burris, 21 M.J. 140, 144 (C.M.A.1985).

#### Disagreement Between Convening Authorities

The military judge incorrectly found as a fact that there was an obvious dispute between the two commanders. There is no support in the record for this finding and we disapprove it. He also incorrectly concluded as a matter of law that the referral of charges by the Superintendent of the Naval Academy was improper because RULES FOR COURTS-MARTIAL 306 and 401, MANUAL FOR COURTS-MARTIAL, UNITED STATES (2002 ed.) required the Superintendent to petition competent superior authority to resolve the alleged dispute between the commanders.

[1] A command other than the one to which the accused is attached may refer charges against the accused to a court-martial. Properly convened courts-martial may try any person subject to the UCMJ. Article 2, UCMJ, 10 U.S.C. § 802; R.C.M. 202. The President has stated that "Any convening authority may refer charges to a court-martial convened by that convening authority...." R.C.M. 601(b). Included in the Discussion section under R.C.M. 601(b) is the statement that "[t]he convening authority may be of any command, including a command different from the accused...." The Service Courts have uniformly upheld such personal jurisdiction within each service that transcends command boundaries. United States v. Talty, 17 M.J. 1127, 1130 (N.M.C.M.R.1984); United States v. Kloese, 24 M.J. 783, 785 (A.C.M.R.1987).

There is no indication in either the Manual for Courts-Martial or in case law that one convening authority will have precedence over another in the unusual situation where more than one convening authority refers charges. In that event, the command to which the accused is attached or a superior in the chain of command has, as a practical matter, control over which convening authority will ultimately complete the court-martial by virtue of the power to provide or withhold orders for the accused to appear. This conclusion is suggested by the drafters in the Discussion

60 M.J. 917  
(Cite as: 60 M.J. 917)

section of R.C.M. 601(b), which states that, "as a practical matter the accused must be subject to the orders of the convening authority or otherwise under the \*920 convening authority's control to assure the appearance of the accused at trial."

The drafters of the Manual further state that the convening authority's control over the accused may be based on an agreement between the commanders involved. *Id.* In the event that a convening authority who is frustrated by not having control over the accused is dissatisfied with the manner in which the case is handled, that commander may elevate the matter to the first common superior to both commands, who should resolve the disagreement between the subordinate commanders. See R.C.M. 401(a); R.C.M. 601(f); see also *United States v. Blaylock*, 15 M.J. 190, 193-94 (C.M.A.1983).

Assuming arguendo that a requirement to petition higher authority exists in law, here there was no disagreement between the Superintendent of the Naval Academy and the Commander, MCB, Quantico, regarding resolution of this case. The Commander, MCB, Quantico, reviewed the report of investigation and used his independent judgment not to re-refer the charges following their withdrawal from the original court-martial. The Superintendent, in like fashion, reviewed the same report of investigation and used his independent judgment to refer charges to his own properly convened court-martial. The disagreement, had there been one, would have come as a result of the Commander, MCB, Quantico, refusing to make the appellee available for trial, as the appellee was not then subject to the orders of the Superintendent. R.C.M. 601(b).

Here, the commanders had an agreement that the accused would be made available for trial in the event the charges were referred to trial by the Superintendent. Had the Commander, MCB, Quantico, refused to make the accused available (and this court can find no requirement that he was obligated to do so), the Superintendent's only recourse would have been to seek the intervention of the next superior in command common to both, the Secretary of the Navy.

#### Improper Re-referral of Charges

[2] The military judge also found that the re-referral of the offenses was improper because the later referral was more onerous and, therefore, R.C.M.

604(b) required that the reasons for the withdrawal and re-referral of charges be included in the record.

Appellate Exhibit XVII. "When charges which have been withdrawn from a court-martial are referred to another court-martial, the reasons for the withdrawal and later referral should be included in the record of the later court-martial, if the later referral is more onerous to the accused." R.C.M. 604(b), Discussion. The military judge found the addition of offenses involving forcible sodomy to be more onerous than the original set of charges facing the accused. Appellate Exhibit XVII.

Our superior court established that the language the military judge relied on in dismissing the offenses creates a requirement that can, standing alone, act as a bar to proper subsequent referral. "Therefore, we will require, for all trials beginning on or after the effective date of this decision, an affirmative showing on the record of the reason for withdrawal and rereferral of any specification." *United States v. Hardy*, 4 M.J. 20, 25 (C.M.A.1977). While later decisions of that court have questioned the "pedigree" of the decision in *Hardy*, it remains binding precedent on this court. *United States v. Koke*, 34 M.J. 313, 314 n. 2 (C.M.A.1992). Interestingly, the language in *Hardy* does not expressly limit its application to charges where the subsequent referral is more onerous to the accused, but read in context with the Discussion to R.C.M. 604(b) and related cases, such a limitation would appear to be implied.

In conducting his analysis, the military judge skipped a foundational step, determining whether, in fact, the charges referred by the Superintendent were the same charges previously referred for trial by the Commanding General, MCB, Quantico.

The following offenses were referred for trial by the Commanding General, MCB, Quantico, on 26 March 2003:

Charge 1, Specification 1, Article 92, Violation of U.S. Navy Regulation 1165 (fraternization)\*921 with (Midshipman Third Class) MIDN 3/C "T");

Charge 1, Specification 2, Article 92, Violation of U.S. Navy Regulation 1165 (fraternization with MIDN 3/C "G");

60 M.J. 917  
(Cite as: 60 M.J. 917)

Charge II, Specification, Article 128, Assault Consummated by Battery (touched shoulder of Second Lieutenant (2ndLt) "R");

Charge III, Specification 1, Article 134, Drunk and Disorderly on 21 June 2001;

Charge III, Specification 2, Article 134, Drunk and Disorderly on 26 April 2002;

Charge III, Specification 3, Article 134, Indecent Language toward 2ndLt "R"; and,

Charge III, Specification 4, Article 134, Solicit 2ndLt "S" to commit an offense.

#### Enclosure 2 of Appellate Exhibit II.

The Superintendent of the Naval Academy referred the following offenses on 12 March 2004 for trial:

Charge I, Specification 1, Article 92, Violation of SECNAVINST 5300.26C (verbal sexual harassment of then Midshipman First Class (MIDN 1/C) "R");

Charge I, Specification 2, Article 92, Violation of SECNAVINST 5300.26C (verbal and physical sexual harassment of then-Midshipman Fourth Class (MIDN 4/C) "T");

Charge I, Specification 3, Article 92, Violation of OPNAVINST 5370.2B (fraternization with then-MIDN 4/C "T");

Charge I, Specification 4, Article 134, Dereliction of Duty (fraternization with then-MIDN 4/C "T");

Charge II, Specification 1, Article 125, Forcible Sodomy with then-MIDN 4/C "T" on 17 November 2001;

Charge II, Specification 2, Article 125, Forcible Sodomy with then-MIDN 4/C "T" on 23 November 2001;

Charge III, Specification I, Article 134, Indecent

Assault on then-MIDN 4/C "T" on 17 November 2001;

Charge III, Specification 2, Article 134, Indecent Assault on then-MIDN 4/C "T" on 23 November 2001; and,

Charge III, Specification 3, Article 134, Drunk and Disorderly on April to May 2002.

#### Charge Sheets; Record at 15.

The original set of charges included the two violations of Navy Regulations on fraternization that were dismissed without prejudice by the military judge in the first court-martial for failure to state an offense. One of these charges was re-referred as a violation of the OPNAVINST governing fraternization. This is a proper re-referral because the re-referral is not more onerous than the original referral and, in any event, reasons for the dismissal, failure to state an offense, are a matter of record at the second court-martial. Dismissal of a specification for failure to state an offense does not ordinarily bar re-referral of the offense if the grounds for the dismissal no longer exist. R.C.M. 907(a), Discussion.

The two specifications of forcible sodomy, two specifications of sexual harassment, and two specifications of indecent assault referred for trial by the Superintendent of the Naval Academy were not previously referred to a court-martial. As the testimony and evidence on the motion in the second court-martial attest, the original convening authority did not consider the evidence sufficient to refer charges of forcible sodomy or indecent assault. This is based on the convening authority's determination that the evidence supported only consensual sexual activity. Because these charges were never referred to trial by the original convening authority, the Superintendent of the Naval Academy was free to refer them to court-martial without explanation under R.C.M. 601(b), and R.C.M. 604(b) does not bar that referral.

The only remaining offense, drunk and disorderly conduct, was referred to trial by the original convening authority and subsequently withdrawn prior to October of 2003. The re-referral of this specification is not more onerous than the original referral, as it was referred on both occasions to a special \*922 court-martial. Therefore, the requirement in R.C.M.

60 M.J. 917  
(Cite as: 60 M.J. 917)

604(b) that the reasons for the withdrawal and re-referral be made a matter of record does not apply to this specification.

**Decision**

The Government appeal is granted. The record of trial is returned to the Judge Advocate General for remand to the convening authority for appropriate disposition, including trial.

Senior Judge CARVER and Judge REDCLIFF concur.

N.M.Ct.Crim.App.,2005.  
U.S. v. Jones  
60 M.J. 917

END OF DOCUMENT

**Lind, Denise R COL USARMY (US)**

---

**From:** Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA  
[JoDean.Morrow@jfhqncr.northcom.mil]  
**Sent:** Friday, June 08, 2012 8:52 AM  
**To:** David Coombs; Lind, Denise R COL USARMY (US); Williams, Patricia A CIV (US); Jefferson, Dashawn MSG USARMY (US)  
**Cc:** Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US); Fein, Ashden MAJ USARMY (US); Overgaard, Angel M CPT USARMY (US); Whyte, Jeffrey H CPT USARMY (US); von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA  
**Subject:** RE: Court's Questions (UNCLASSIFIED)

Classification: UNCLASSIFIED

Caveats: NONE

Your Honor - A very brief reply to the Legislative History portion of the Defense Response to the Court's Questions:

As stated by the Government during oral argument, the 1984 legislative history is very clear that "exceeding authorized access" on a computer is not restricted to "breaking" or "bypassing some technical restriction." The United States quoted this passage verbatim:

"It is not difficult to envision an employee or other individual who, while authorized to use a particular computer in one department, briefly exceeds his authorized access and peruses data belonging to the department that he is not supposed to look at."

S. Rep. No. 99-432 at 2485.

Additionally, the definition of "exceeds authorized access" begins by stating "exceeds authorized access means to access a computer with authorization..." The government doesn't understand how that could be interpreted by the defense to mean "breaking" into a computer. The most important point from the section you referred the defense and government to during oral argument is that which states:

"[S]ection 1030(a)(1) would require proof that the individual knowingly used a computer without authority, or in excess of authority, for the purpose of obtaining classified information."

Again, 1030(a)(1) prohibits individuals from accessing a computer in excess of authority for the purpose of obtaining classified information.

Respectfully,

CPT Joe Morrow  
Trial Counsel  
U.S. Army Military District of Washington  
Phone: 202-685-1975  
NIPR: [jodean.morrow@jfhqncr.northcom.mil](mailto:jodean.morrow@jfhqncr.northcom.mil)  
SIPR: [jodean.morrow@jfhqncr.northcom.smil.mil](mailto:jodean.morrow@jfhqncr.northcom.smil.mil)

-----Original Message-----

From: David Coombs [<mailto:coombs@armycourt martialdefense.com>]  
Sent: Thursday, June 07, 2012 9:46 PM  
To: Lind, Denise R COL USARMY (US); Williams, Patricia CIV JFHQ-NCR/MDW SJA; Jefferson, Dashawn MSG USARMY (US)

Cc: Hurley, Thomas F MAJ USARMC (US); 'Tooman, Joshua J CPT USARMC (US)'; Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA  
Subject: Court's Questions

Ma'am,

The Court had several questions for the Defense during today's motions argument. In particular, the Court asked the Defense the following questions:

- 1) What is the Court's authority to dismiss the 1030 offenses?
- 2) How does the Defense interpret the passage quoted by the Court from the legislative history of section 1030?
- 3) Does the elements test require a Court to look at the elements as charged or simply the statutory elements?

The Defense has provided further responses in the Attachment (and has provided a case in support of the Court's authority to dismiss the 1030 offenses).

Best,

David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906

Toll Free: 1-800-588-4156

Local: (508) 689-4616

Fax: (508) 689-9282  
[coombs@armycourtartialdefense.com](mailto:coombs@armycourtartialdefense.com)  
<<mailto:coombs@armycourtartialdefense.com>>

[www.armycourtartialdefense.com](http://www.armycourtartialdefense.com) <<http://www.armycourtartialdefense.com/>>

\*\*\*Confidentiality Notice: This transmission, including attachments, may contain confidential attorney-client information and is intended for the person(s) or company named. If you are not the intended recipient, please notify the sender and delete all copies. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited.\*\*\*

Classification: UNCLASSIFIED

Caveats: NONE



IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC  
U.S. Army, xxx-xx-  
HHC, U.S. Army Garrison  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211 )

) **RULING: DEFENSE MOTION  
TO DISMISS SPECIFICATIONS  
2, 3, 5, 7, 9, 10, 11 AND 15 OF  
CHARGE II**

) DATED: 8 June 2012

Defense moves this Court to dismiss Specifications 2, 3, 5, 7, 9, 10, 11, and 15 of Charge II as unconstitutionally vague in violation of the Fifth Amendment and overbroad in violation of the First Amendment. Alternatively, Defense moves the Court to provide limiting instructions. Government opposes dismissal. The Government joins the Defense in its request to provide instructions that define 18 U.S.C. § 793(e). After considering the pleadings, evidence presented, and argument of counsel, the Court finds and concludes the following:

**Factual Findings:**

1. In Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II, PFC Manning is charged with unauthorized possession and disclosure of classified information in violation of 18 U.S.C. Section 793(e) and Article 134, UCMJ.
2. 18 U.S.C. § 793(e) criminalizes "[w]hoever having unauthorized possession of, access to control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it."

**The Law: Void for Vagueness.**

1. A motion to dismiss a specification as being "void for vagueness" implicates the Due Process clause of the Fifth Amendment. To overcome a "void for vagueness challenge," a statute must be reasonably clear so as to provide warning of the type of conduct which is proscribed and provide standards sufficiently explicit to prevent arbitrary and capricious application. A statute is impermissibly vague if it "(1) fails to provide people of ordinary intelligence a reasonable opportunity to understand what conduct it prohibits; or (2) authorizes or even encourages

arbitrary and discriminatory enforcement.” *U.S. v. Shrader*, 2012 WL 1111654 (4<sup>th</sup> Circuit, 4 April 2012) quoting *Hill v. Colorado*, 530 U.S. 703, 732 (2000); *U.S. v. Amazaki*, 67 M.J.666 (A. Ct. Crim. App. 2009). “[T]he more important aspect of vagueness doctrine is not actual notice, but the other principal element of the doctrine—the requirement that a legislature establish minimal guidelines to govern law enforcement.” Courts also consider any judicial or administrative limiting construction of a criminal statute in determining whether it is unconstitutionally vague. *Kolendar v. Lawson*, 461 U.S. 352, 355, 357, 358 (1983).

2. A person to whom a statute clearly applies has no standing to challenge successfully the statute under which he was charged for vagueness, *U.S. v. Morison*, 844 F.2d 1057 (4<sup>th</sup> Cir. 1988).

3. A *mens rea* requirement mitigates a law’s vagueness especially with respect to actual notice of the conduct proscribed. *U.S. v. Moyer*, 2012 WL 639277 (3<sup>rd</sup> Cir. 2012) quoting *Gonzales v. Cartwright*, 550 U.S. 124, 149 (2007).

#### **The Law: Substantially Overbroad.**

1. A statute is facially overbroad when no set of circumstances exists under which it would be valid. *United States v. Salerno*, 481 U.S. 739, 745 (1987).

2. In the First Amendment context, a statute is “overbroad” when a substantial number of its applications are unconstitutional when compared with the statute’s plainly legitimate sweep. *U.S. v. Stevens*, 130 S. Ct. 1577 (2010). First Amendment overbreadth challenges are an exception to the general rule that an accused does not have standing to litigate the rights of 3<sup>rd</sup> parties. *U.S. v. Morison*, 844 F.2d 1057 (4<sup>th</sup> Cir. 1988).

#### **Analysis: Void for Vagueness – Phrase “Relating to the National Defense.”**

1. The phrase “relating to the national defense” is not defined in the statute. Defense argues the phrase is unconstitutionally vague because it gives no fair warning of what information comes within its sweeping scope.

2. In *Gorin v. United States*, 312 U.S. 19 (1941), the Supreme Court rejected a similar vagueness challenge to identical language in the Espionage Act, the predecessor to the statute at issue in this case. The Court held:

National defense, the Government maintains, ‘is a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness.’ We agree that the words ‘national defense’ in the Espionage Act carry that meaning.....The language employed appears sufficiently definite to apprise the public of prohibited activities and is consonant with due process. *Gorin*, at 28.

3. Post-*Gorin* federal courts have consistently found that the phrase “relating to the national defense” in 18 U.S.C. section 793 is not unconstitutionally vague. See *U.S. v. Morison*, 844 F.2d 1057, 1071-1074 (4<sup>th</sup> Cir. 1988); *United States v. Kim*, 808 F. Supp. 2d 44 (D.D.C. 2011); *United*

*States v. Rosen*, 445 F. Supp. 2d 602, 617-22 (E.D. Va. 2006), aff'd on other grounds, 557 F.3d 192 (4<sup>th</sup> Cir. 2009).

4. The Court agrees with the analysis in these cases and finds the phrase "relating to the national defense" in 18 U.S.C. 793(e) is not unconstitutionally vague.

**Analysis: Void for Vagueness – Phrase "to the Injury of the United States or to the Advantage of Any Foreign Nation."**

1. 18 U.S.C. Section 793(e) imposes an additional *scienter* requirement for transmission of information requiring that the accused "has reason to believe the national defense information could be used to the injury of the United States or to the advantage of any foreign nation."

2. The Supreme Court rejected a vagueness challenge to the predecessor statute on the basis of "the obvious delimiting words in the statute" requiring that defendants act with "intent or reason to believe that the information to be obtained is to be used to the injury of the United States or to the advantage of any foreign nation." *Gorin*, at 28-29. As a result, the Court found "no uncertainty in [the] statute which deprives a person of the ability to predetermine whether a contemplated action is criminal under the provisions of this law." *Id.* at 28.

3. The statute requires the accused to have acted "willfully. This *scienter* requirement the statute imposes when an individual is charged with transmitting "information relating to the national defense" mitigates the law's vagueness especially with respect to actual notice of the conduct proscribed. See *U.S. v. Ragen*, 314 U.S. 513, 524 (1942); *U.S. v. Kim*, 808 F. Supp. 2d 44 (D.D.C. 2011), *U.S. v. Moyer*, 2012 WL 639277 (3<sup>rd</sup> Cir. 2012) quoting *Gonzales v. Cartwright*, 550 U.S. 124, 149 (2007).

4. The Court agrees with the analysis in these cases and finds the phrase "to the injury of the United States or to the Advantage of any Foreign Nation" in 18 U.S.C. 793(e) is not unconstitutionally vague.

5. For the reasons set forth above, the Court finds that the combination of the phrases "relating to the national defense" and "to the Injury of the United States or to the Advantage of Any Foreign Nation" does not render the statute unconstitutionally vague.

6. Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II are not unconstitutionally vague. Vagueness concerns can be addressed with appropriate instructions. *U.S. v. Squillacote*, 221 F.3d 542 (4<sup>th</sup> Cir. 2000).

**Analysis: Substantially Overbroad in Violation of the 1<sup>st</sup> Amendment.**

1. Defense argues that 18 U.S.C. Section 793(e) is substantially overbroad in violation of the 1<sup>st</sup> Amendment because it regulates a substantial amount of protected speech and infringes on the freedom of the press to investigate and publish articles on national defense topics.

2. A similar overbreadth challenge was litigated in *U.S. v. Morison*, 844 F.2d 1057 (1988). The *Morison* court applied a 3 prong test to determine whether 18 U.S.C. 793(e) was overbroad in violation of the First Amendment: (1) is the government interest sought to be implemented too insubstantial or at least insufficient in relation to the inhibitory effects on First Amendment freedom? (2) do the means bear little relation to the asserted government interest? and (3) if the means do relate to a substantial government interest, can that interest be achieved by a method less invasive of free speech interests? The 4<sup>th</sup> Circuit held that 18 U.S.C. 793(e) - (1) expresses a vital government interest in protecting national security; (2) the statute has a direct relation to the protection of the vital national security interest; and (3) judicial instructions can narrow the scope of a statute to ensure the statute is narrowly tailored to protect the vital national security interest.

3. The Court agrees with the 4<sup>th</sup> Circuit that 18 U.S.C. 793(e) expresses a vital government interest in protecting national security and that the statute has a direct relation to the protection of the vital national security interest. This Court can craft instructions to ensure that the statute is narrowly tailored to protect the vital national security interest.

4. Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II are not unconstitutionally overbroad in violation of the First Amendment.

**Conclusion.** Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II are not unconstitutionally vague nor substantially overbroad. The Court will provide appropriate instructions to fully inform the fact-finder of the elements of the offense and its definitions. The parties are invited to provide the Court with proposed instructions. The Court would greatly benefit from the actual instructions used to define elements and definitions in previous 18 U.S.C. 793 cases, to include *U.S. v. Kim*, 808 F. Supp.2d 44 (D.D.C. 2011); *U.S. v. Rosen*, 445 F.Supp. 2<sup>nd</sup> 602 (E.D. Va. 2006); *U.S. v. Squillacote*, 221 F.3d 542 (4<sup>th</sup> Cir. 2000); *U.S. v. Morison*, 844 F.2d 1057 (4<sup>th</sup> Cir. 1988); *U.S. v. Truong Dinh Hung*, 629 F.2d 908 (4<sup>th</sup> Cir. 2000); and *U.S. v. Dedeyan*, 584 F.2d 36 (4<sup>th</sup> Cir. 1978).

**RULING:** Defense Motion to Dismiss Specifications 2, 3, 5, 7, 9, 10, 11 and 15, of Charge II is **DENIED**. The Court will draft instructions similar to those approved by the Fourth Circuit and invites the parties to submit proposed instructions for consideration.

**ORDERED**, this the 8<sup>th</sup> day of June 2012.



DENISE R. LIND  
COL, JA  
Chief Judge, 1st Judicial Circuit

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, xxx-xx- )

Headquarters and Headquarters Company, )

U.S. Army Garrison, Joint Base Myer- )

Henderson Hall, Fort Myer, VA 22211 )

**RULING: DEFENSE MOTION:  
DISMISS SPECIFICATIONS 13  
AND 14 OF CHARGE II - FAIL  
TO STATE AN OFFENSE**

**DATED: 8 June 2012**

Defense moves the Court to dismiss Specifications 13 and 14 of Charge II for failure to state an offense because the Government has failed to allege the Accused's conduct exceeded unauthorized access within the meaning of 18 U.S.C. Section 1030(a)(1). Government opposes. After considering the pleadings, evidence presented, and argument of counsel, the Court finds and concludes the following:

**Factual Findings:**

1. Specifications 13 and 14 of Charge II charge PFC Manning with violating 18 U.S.C. Section 1030(a)(1) and Article 134, UCMJ.
2. Specification 13 of Charge II alleges that the accused:

did, at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010, having knowingly exceeded authorized access on a Secret Internet Protocol Router Network computer, and by means of such conduct having obtained information that has been determined by the United States government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, to wit: more than seventy-five classified United States Department of State cables, willfully communicate, deliver, transmit, or cause to be communicated, delivered, or transmitted the said information, to a person not entitled to receive it, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, in violation of 18 U.S. Code Section 1030(a)(1) such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces.

3. Specification 14 of the same charge alleges that the accused:

did, at or near Contingency Operating Station Hammer, Iraq, between on or about 15 February 2010 and on or about 18 February 2010, having knowingly exceeded authorized access on a Secret Internet Protocol Router Network Computer, and by means of such conduct having obtained that has been determined by the United States government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, to wit: a classified Department of State cable titled "Reykjavik-13", willfully communicate, deliver, transmit, or cause to be communicated, delivered, or transmitted the said information, to a person not entitled to receive it, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, in violation of 18 U.S. Code Section 1030(a)(1) such conduct being prejudicial to good order and discipline in the armed forces and being of a nature to bring discredit upon the armed forces.

3. Defense avers that the Government theory at trial will be either that: (1) PFC Manning exceeded authorized access when he allegedly accessed information for an improper purpose (to give it to someone not entitled to receive it); or (2) that PFC Manning exceeded authorized access when he allegedly accessed, stored, and disclosed information in contravention of the Army's acceptable use policy (AUP). The Government asserted during oral argument that it will be presenting evidence in addition to the (AUP) to prove that the accused exceeded authorized access.

4. During the Article 32 Investigation, Special Agent David Shaver from the U.S. Army Computer Crimes Investigative Unit testified that he examined the two Secret Internet Protocol Router Network (SIPRNET) computers used by the accused from approximately October 2009 through May 2010. (Gov't Enclosure 1, pp. 125-7). Special Agent Shaver testified when logging into both computers, the user is presented with a warning banner. *Id.* at 134-5.

5. The warning banner states as follows:

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC, monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence investigations. At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception and search, and may

be disclosed or used for any USG authorized purpose. This IS includes security measures (e.g. authentication and access controls) to protect USG-interests—not for your personal benefit or privacy. Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content [sic] of privileged [sic] communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement or details.

(Gov't Enclosure 2.)

6. In January 2011, Special Agent Mark Mander from U.S. Army Computer Crime Investigative Unit interviewed Captain (CPT) Thomas Cherepko, from Headquarters and Headquarters Company, 2<sup>nd</sup> Brigade Combat Team, 10<sup>th</sup> Mountain Division, who was the Assistant S-6 Officer during the time the accused was stationed in Iraq. (Gov't Enclosure 5, p. 1) CPT Cherepko stated that a signed user agreement for each user was required to access SIPRNET; however, he could not locate a copy of accused's signed user agreement. *Id.*

7. Defense does not contest that specifications 13 and 14 allege every element of the offense charged, 18 U.S.C. Section 1030(a)(1) and Article 134 UCMJ. Defense challenges the theory underlying the specification as deficient. Such a challenge has been styled a "failure to state an offense" in Federal Courts under Federal Rule of Criminal Procedure 12 and, where the Government theory is undisputed, the Court can address and dismiss the charge prior to trial. See *U.S. v. Nosal*, 2012 WL 1176119 (9<sup>th</sup> Cir. 2012).

#### **The Law: Failure to State an Offense.**

1. The military is a notice pleading jurisdiction. A charge and its specification is sufficient if it (1) contains the elements of the offense charged and fairly informs an accused of the charge against which he must defend; and (2) enables the accused to plead an acquittal or conviction in bar of future prosecutions for the same offense. In reviewing the adequacy of a specification, the analysis is limited to the language as it appears in the specification, which must expressly allege the elements of the offense or do so by necessary implication. *U.S. v. King*, 71 M.J. 50, fn 2, (C.A.A.F. 2012), quoting *U.S. v. Fosler*, 70 M.J. 225, 229 (C.A.A.F. 2011) and *U.S. v. Fleig*, 16 C.M.A. 444, 445 (1966) (looking "within the confines of the specification"). A motion to dismiss for failure to state an offense is a challenge to the adequacy of a specification and whether the specification "alleges, either expressly or by implication, every element of the offense, so as to give the accused notice and protection against double jeopardy." *United States v. Amazaki*, 67 M.J. 666, 669, 670 n.8 (A. Ct. Crim. App. 2009) (quoting *United States v. Crafter*, 64 M.J. 209, 211 (C.A.A.F. 2006)).

#### **The Law: The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(1).**

1. An accused violates the Computer Fraud and Abuse Act (CFAA) when the accused

knowingly accessed a computer without authorization or *exceeding authorized access*, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it. 18 U.S.C. §1030(a)(1)(emphasis added) .

2. 18 U.S.C. § 1030(e)(6) defines the phrase “exceeds authorized access” as “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter.”

### **Analysis: Statutory Interpretation**

1. The crux of the Defense motion is the interpretation of the “exceeds authorized access” language in the CFAA. Defense argues that the Government failed to allege that he “exceeded authorized access” within the meaning CFAA because he was authorized to access the SIPRNET and entitled to access the classified information in question. The Government has alleged in the specification that the accused “exceeded authorized access”. The Government further avers that it will prove the accused “exceeded authorized access” by the AUP and by other evidence.

2. In *United States v. Starr*, 51 M.J. 528, 532 (A.F. Ct. Crim. App. 1999), the Air Force Court of Criminal Appeals provided a roadmap to resolving the legal meaning of a statute:

It is the function of the legislature to make the laws and the duty of judges to interpret them. 2A Norman J. Singer, Sutherland Statutory Construction § 45.03 (4th ed. 1984). Judges should interpret a statute so as to carry out the will of the legislature. *United States v. Dickenson*, 20 C.M.R. 154, 165 (C.M.A. 1955). Otherwise, they violate the principle of the separation of powers. Singer, *supra*, § 45.05. “If the words used in the statute convey a clear and definite meaning, a court has no right to look for or to impose a different meaning.” *Dickenson*, 20 C.M.R. at 165. Thus, in interpreting a statute, we employ the following process: (1) Give the operative terms of the statute their ordinary meaning; if the terms are unambiguous, the inquiry is over; (2) If the operative



terms of the statute are ambiguous, then we examine the purpose of the statute as well as its legislative history; and (3) If a reasonable ambiguity still exists, then we apply the rule of lenity and resolve the ambiguity in favor of the accused.

### **CFAA: Ordinary Meaning of the Statute**

As discussed in further detail below, the term “exceeds authorized access” has been subject to differing interpretations among the U.S. Circuit Courts of Appeals thereby indicating that the statutory language is not clear and definite. *Compare Nosal III*, 2012 W.L. 1176119 with *United States v. John*, 597 F.3d 263 (5th Cir. 2010) and *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2007). Therefore, because the ordinary meaning of the operative language is ambiguous, the Court must look to the purpose of the statute and statutory history. *Starr*, 51 M.J. at 532.

### **CFAA: Legislative History.**

1. The CFAA was originally enacted in 1984. Act of Oct. 12, 1984, Pub. L. No. 98-473, §§ 2101-2103, 98 Stat. 1837, 2190-92. In its original version, Section 1030(a)(1) punished anyone who

knowingly accesses a computer without authorization, *or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend*, and by means of such conduct obtains information that has been determined by the United States Government . . . to require protection against unauthorized disclosure for reasons of national defense or foreign relations . . . with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation.

*Id.* § 2102(a), 98 Stat. 2190 (emphasis supplied).

2. Two years later in 1986, Congress replaced the terms “or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend” with the terms “or exceeds authorized access.” Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2(c), 100 Stat. 1213. As the Senate Report for the 1986 bill explained:

Section 2(c) [of the 1986 bill] substitutes the phrase ‘exceeds authorized access’ for the more cumbersome phrase in present 18 U.S.C. § 1030(a)(1) and (2), ‘or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend’. The Committee intends this change to simplify the language in 18 U.S.C. § 1030(a)(1) and (2), and the phrase ‘exceeds authorized access’ is defined separately in Section 2(g) of the bill.

S. Rep. No. 99-432, pt. 3, *reprinted in* 1986 U.S.C.C.A.N. 2479, 2486.

3. Additionally, Congress added to Section 1030 the definition of “exceeds authorized access” that is presently codified at § 1030(e)(6). *Id.* § 2(g)(4); *see* 18 U.S.C. § 1030(e)(6). However, in its attempt to simplify the language, Congress changed the scope of the statute:

Further, the legislative purpose and history supports the plain meaning of the statute. Congress enacted the CFAA to deter “the criminal element from abusing computer technology in future frauds.” H.R.Rep. No. 98–894, at 4 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3690. As originally enacted, the CFAA applied to a person who (1) knowingly accessed without authorization or (2) “having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend.” Pub.L. No. 98–473, § 2102, 98 Stat. 2190, 2190–91 (1984). Congress amended the statute by replacing the latter means of access with the phrase “exceeds authorized access.” *See* Pub.L. No. 99–474, § 2, 100 Stat. 1213, 1213 (1986). The stated reason for the amendment was to simplify the language in 18 U.S.C. 1030(a)(1) and (2).

4. In 1996, Congress amended 18 U.S.C. § 1030(a)(1) and clarified the differences between the CFAA and federal espionage statutes:

Although there is considerable overlap between 18 U.S.C. [§] 793(e) and [§] 1030(a)(1), as amended by the NII Protection Act, the two statutes would not reach exactly the same conduct. [§] 1030(a)(1) would target those persons who deliberately *break into a computer* to obtain properly classified Government secrets then try to peddle those secrets to others, including foreign governments. In other words, unlike existing espionage laws prohibiting the theft and peddling of Government secrets to foreign agents, [§] 1030(a)(1) would require proof that the individual knowingly used a computer without authority, or in excess of authority, for the purpose of obtaining classified information. In this sense then, it is the use of the computer which is being proscribed, not the unauthorized possession of, access to, or control over the classified information itself.

S. Rep. No. 104-357 at 6-6 (1996) (emphasis added).

5. Therefore, an analysis of the legislative history of the CFAA and the phrase “exceeds authorized access” reveals that the statute is not meant to punish those who use a computer for an improper purpose or in violation the governing terms of use, but rather the statute is designed to

criminalize electronic trespassers and computer hackers. See *Int'l Ass'n of Machinists & Aerospace Workers*, 390 F. Supp. 2d at 495 (quoting *Sherman & Co. v. Salton Maxim Housewares, Inc.*, 94 F. Supp. 2d 817, 820 (E.D. Mich. 2000)).

### **CFAA: Case Law and Conflict Among the Federal Circuits.**

1. In *Nosal III*, at 856, the appellant convinced his former co-workers at his previous firm, Korn/Ferry, to help him establish a competing business. The former co-workers used their Korn/Ferry log-in credentials to download information from a confidential database. They then passed this information to the appellant. The former co-workers “were authorized to access the database, but Korn/Ferry had a policy that forbade disclosing confidential information.” The Defendant was charged, *inter alia*, with violations of 18 U.S.C. § 1030(a)(4), for aiding and abetting the Korn/Ferry employees in “exceed[ing their] authorized access” with intent to defraud.” The appellant filed a motion to dismiss the CFAA charges, “arguing that the statute targets only hackers, not individuals who access a computer with authorization but then misuse information they obtain by means of such access. *Id.*”

2. The Court, in *Nosal III* at 857, agreed with the appellant’s argument and disagreed with the prosecution’s attempt to make the CFAA into “an expansive misappropriation statute” when it was originally was created as “an anti-hacking statute.” To support its conclusion, the *Nosal III* Court cited the legislative purpose of the CFAA:

Congress enacted the CFAA in 1984 primarily to address the growing problem of computer hacking, recognizing that, “[i]n intentionally trespassing into someone else’s computer files, the offender obtains at the very least information as to how to break into that computer system.” S.Rep. No. 99-432, at 9 (1986), 1986 U.S.C.A.N. 2479, 2487 (Conf. Rep.). *Id.* at 858.

3. The *Nosal III* Court, in the end, held that the terms “‘exceed authorized access’ in the CFAA [and as defined by 18 U.S.C. § 1030(e)(6)] does not extend to violations of use restrictions.” *Id.* at 863. *Nosal III* defines “exceeds unauthorized access” to apply to *inside* hackers or individuals whose initial access to a computer is authorized but who accesses unauthorized information or files.

4. The *Nosal III* Court, at 862, also acknowledged that its ruling differed from previous decisions made by other circuits namely *United States v. John*, 597 F.3d 263 (5th Cir. 2010) (“Exceeds authorized access” occurred when the appellant violated her employer’s official policy by misusing the company’s internal computer when she properly accessed the computer system and customer account information contained in it, but provided the information to others who were able to incur fraudulent charges.) and *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2007) (“Exceeds authorized access” occurred when the appellant violated his agency’s policy of only obtaining information from its databases for official reasons by properly accessing the agency’s computer system, but obtaining personal information from seventeen different individuals for personal reasons.) However, the *Nosal III* Court reasoned that its sister circuits incorrectly looked at the culpable actions of the appellants and did not consider the negative

effects of expanding the definition of “exceeds authorized access” to include “violations of corporate computer use restrictions or violations of a duty of loyalty.”

5. Other court decisions support the *Nosal III* Court’s narrow view of “exceeds authorized access.” See *Orbit One Commc’ns, Inc. v. Numerex Corp.*, 692 F.Supp.2d 373, 385 (S.D.N.Y.2010); *United States v. Aleynikov*, 737 F. Supp. 2d 173, 192 (S.D.N.Y. 2010); *Diamond Power Int’l, Inc. v. Davidson*, 540 F.Supp.2d 1322, 1343 (N.D.Ga.2007); *Shamrock Foods Co. v. Gast*, 535 F.Supp.2d 962, 965 (D.Ariz.2008); *Int’l Ass’n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F.Supp.2d 479, 499 (D.Md.2005) .

### **Rule of Lenity.**

1. When construing ambiguous criminal statutes, military courts have consistently applied the rule of lenity. See *United States v. Schelin*, 15 M.J. 218, 220 (C.M.A. 1983); *United States v. Cartwright*, 13 M.J. 174, 176 & n.4 (C.M.A. 1982); *United States v. Inthavong*, 48 M.J. 628, 630 (A. Ct. Crim. App. 1998). “[T]he rule of lenity, which is rooted in considerations of notice, requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government.” *United States v. Romm*, 455 F.3d 990, 1001 (9th Cir. 2006).

2. When applying the Rule of Lenity in the CFAA context, the *Nosal III* Court stated at 863:

If Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly. The rule of lenity requires “penal laws . . . to be construed strictly.” *United States v. Wiltberger*, 18 U.S. (5 Wheat.) 76, 95, 5 L.Ed. 37 (1820). “[W]hen choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite.” *Jones [v. United States]*, 529 U.S. [848,] 858, 120 S.Ct. 1904 [(2000)] (internal quotation marks and citation omitted)...This narrower interpretation is also a more sensible reading of the text and legislative history of a statute whose general purpose is to punish hacking – the circumvention of technological access barriers – not misappropriation of trade secrets – a subject Congress has dealt with elsewhere . . . . Therefore, we hold that “exceeds authorized access” in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*.

### **Conclusions of Law: Failure to State an Offense.**

1. The language of Specifications 13 and 14 of Charge II includes all of the elements of the offense, fairly informs the accused of the charge against which he must defend, and protects the accused against double jeopardy. See *King*, at 51, fn 2; *Fosler*, at 229; *Fleig*, at 445.

2. Federal cases dismissing charges before evidence is presented do so under Federal Rule of Criminal Procedure 12. This court has the power to do the same under R.C.M. 907(b)(1). Whether the Court should dismiss the specifications before presentation of the evidence depends on whether the issue is capable of resolution without trial on the issue of guilt. In this case, the Government stated in oral argument that it would present evidence in addition to the AUP. The Court does not find that the issue is capable of resolution prior to presentation of the evidence. This issue is appropriately decided after presentation of the evidence either as a motion for a finding of not guilty under R.C.M. 917 or a motion for a finding that the evidence is not legally sufficient. *King*, 71 M.J. 50; *U.S. v. Griffith*, 27 M.J. 42 (C.M.A. 1988).

3. The language of the specifications states an offense.

**Conclusions of Law: CFAA.**

1. Applying the Rule of Lenity, the Court shall adopt the narrow meaning of “exceeds authorized access” under the CFAA and instruct the fact finder that the term “exceeds authorized access” is limited to violations of restrictions on *access* to information, and not restrictions on its “use”. The Court shall craft instructions for defining “exceeding authorized access” in Specifications 13 and 14 of Charge II using the language in the legislative history in 1996.

2. Should the Government not prove an element as alleged in the specifications in accordance with the instructions given in accordance with the narrow view of *Nosal III* at the close of the evidence, the Court shall entertain motions under R.C.M. 917 or for a finding that the evidence is not legally sufficient to sustain a guilty finding.

**RULING:** The Defense Motion to dismiss Specifications 13 and 14 of Charge II for failure to state an offense is **DENIED**.

So **ORDERED**: this 8<sup>th</sup> day of June 2012.



DENISE R. LIND  
COL, JA  
Chief Judge, 1st Judicial Circuit

Appellate Exhibit 140

4 pages

classified

"SECRET"

ordered sealed for Reason 2  
and Reason 7 (government)

Military Judge's Seal Order  
dated 20 August 2013

stored in the classified  
supplement to the original  
Record of Trial

Appellate Exhibit 140

Enclosure

4 pages

classified

"SECRET"

ordered sealed for Reason 2  
and Reason 7 (government)

Military Judge's Seal Order

dated 20 August 2013

stored in the classified  
supplement to the original  
Record of Trial

Appellate Exhibit 141

1 page

classified

"SECRET"

ordered sealed for Reason 2  
and Reason 7 (government)

Military Judge's Seal Order  
dated 20 August 2013

stored in the classified  
supplement to the original  
Record of Trial



UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**RULING:**  
**DELAY OF COURT'S RULING**  
**ON DEFENSE MOTION TO**  
**COMPEL DISCOVERY #2**

**DATED: 8 June 2012**

The Government has requested thirty (30) days to delay the Court's ruling on the Defense Motion to Compel Discovery #2 in order to search for the records concerning the Department of State requested by the defense in its Addendum to Defense Motion to Compel Discovery #2. The defense does not object to this request.

**Factual Findings:**

1. On 7 June 2012, three Department of State witnesses, specifically Ms. Marguerite Coffey, Ms. Rena Bitter, and Ms. Catherine Brown, testified during a motions hearing in the above captioned courts-martial. The witnesses referenced the below records in their testimony. The witnesses testified that they were unaware whether the below records remain in existence.

(1) written assessments produced by the Chiefs of Mission used to formulate a portion of the draft damage assessment completed in August of 2011;

(2); written Situational Reports produced by the WikiLeaks Working Group between roughly 28 November 2010 and 17 December 2010;

(3) written minutes and agendas of meetings by the Mitigation Team;

(4) Information Memorandum for the Secretary of State produced by the WikiLeaks Persons at Risk Group;

(5) a matrix produced by the WikiLeaks Persons at Risk Group to track identified individuals;

(6) formal guidance produced by the WikiLeaks Persons at Risk Group and provided to all embassies, including authorized actions for any identified person at risk;

(7) information collected by the Director of the Office of Counterintelligence within the Department of State (DoS) regarding any possible impact from the disclosure of diplomatic cables; and

(8) any prepared written statements for the DoS's reporting to Congress on 7 and 9 December 2010.

2. On 7 June 2012, the Government requested the Court delay the Court's ruling for thirty (30) days on the Defense Motion to Compel Discovery #2, for information pertaining to the Department of State, in order to search for the above referenced records.

3. On 7 June 2012, the defense submitted its Addendum to Defense Motion to Compel Discovery #2 and requested the above records. The defense requested that the prosecution produce this material under Rule for Courts-Martial (RCM) 701(a)(2) or, in the alternative, RCM 703. The defense also requested that the prosecution produce this material under RCM 701(a)(6).

**ORDER:**

1. The Government will **immediately** begin the process of searching for and inspecting the following information:

(1) written assessments produced by the Chiefs of Mission used to formulate a portion of the draft damage assessment completed in August of 2011;

(2) written Situational Reports produced by the WikiLeaks Working Group between roughly 28 November 2010 and 17 December 2010;

(3) written minutes and agendas of meetings by the Mitigation Team;

(4) Information Memorandum for the Secretary of State produced by the WikiLeaks Persons at Risk Group;

(5) a matrix produced by the WikiLeaks Persons at Risk Group to track identified individuals;

(6) formal guidance produced by the WikiLeaks Persons at Risk Group and provided to all embassies, including authorized actions for any identified person at risk;

(7) information collected by the Director of the Office of Counterintelligence within the Department of State (DoS) regarding any possible impact from the disclosure of diplomatic cables; and

(8) any prepared written statements for the DoS's reporting to Congress on 7 and 9 December 2010.

2. By **8 July 2012**, the Government shall **notify** the Court which of the above records exist and, for those records that do exist, file a supplemental response to the Defense's Motion to Compel Discovery #2.

So ORDERED this 8<sup>th</sup> day of June 2012.



DENISE R. LIND

COL, JA

Chief Judge, 1<sup>st</sup> Judicial Circuit

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, xxx-xx- )

Headquarters and Headquarters Company, )

U.S. Army Garrison, Joint Base Myer- )

Henderson Hall, Fort Myer, VA 22211 )

**RULING: DEFENSE AND  
GOVERNMENT MOTIONS FOR  
INSTRUCTIONS ON LESSER  
INCLUDED OFFENSES**

DATED: 8 June 2012

Defense and Government move the Court for instructions on lesser included offenses (LIO). Each party opposes the other's motion, at least in part. After considering the pleadings, evidence presented, and argument of counsel, the Court finds and concludes the following:

**Factual Findings:**

1. The accused is charged with five specifications of violating a lawful general regulation, one specification of aiding the enemy, one specification of conduct prejudicial to good order and discipline and service discrediting, eight specifications of communicating classified information, five specifications of stealing or knowingly converting government property, and two specifications of knowingly exceeding authorized access to a government computer, in violation of Articles 92, 104, and 134, UCMJ, 10 U.S.C. §§ 892, 904, 934.
2. Specifically, in Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II, the accused is charged with authorized possession and disclosure of information relating to the national defense in violation of 18 U.S.C. Section 793(e). In specifications 13 and 14 of Charge II, the accused is charged with knowingly exceeding unauthorized access to a government computer in violation of 18 U.S.C. Section 1030(A)(1). Specification 1 of Charge II charges PFC Manning with wrongfully and wantonly causing United States intelligence to be published on the internet, having knowledge that the intelligence placed on the internet is accessible to the enemy, in violation of Article 134. Finally, Specifications 4, 6, 8, 12, and 16 of Charge II allege that the accused stole, purloined, or knowingly converted to his use or the use of another a thing of value owned by the United States government, with a value over \$1,000 in violation of 18 U.S.C. Section 641. In addition, each of these specifications allege that the conduct described therein is prejudicial to good order and discipline in the armed forces and of a nature to bring discredit upon the armed forces, in violation of Article 134.
3. At the relevant time, Army Regulation 380-5 (Department of the Army Information Security Program) was in effect. The regulation is a punitive lawful general order per paragraph 1-21.
4. As charged, the elements of Specification 1 of Charge II are (1) that the accused wrongfully and wantonly caused to be published on the internet intelligence belonging to the United States

government, having knowledge that intelligence published on the internet is available to the enemy and (2) was of a nature to bring discredit upon the armed forces.

5. As charged, the elements of Specifications 2, 3, 5, 7, 9, 10, 11 and 15 of Charge II, which alleges a violation of 18 U.S.C. § 793(e), are (1) that the accused had unauthorized possession of certain specified information; (2) that the specified information related to the national defense; (3) that the accused had reason to believe the information in question could be used to the injury of the United States or to the advantage of any foreign nation; (4) that the accused willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, the information to any person not entitled to receive it; and (5) that such conduct was prejudicial to good order and discipline in the armed forces and of a nature to bring discredit upon the armed forces.

6. As charged, the elements of Specifications 13 and 14, of Charge II, which alleges a violation of 18 U.S.C. § 1030(a)(1) are (1) that the accused knowingly accessed a computer exceeding authorized access; (2) by means of such conduct having obtained information determined by the United States government by Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations; (3) that the accused had reason to believe the information obtained could be used to the injury of the United States or to the advantage of any foreign nation; (4) that the accused willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, the information to any person not entitled to receive the information; and (5) that such conduct was prejudicial to good order and discipline in the armed forces and of a nature to bring discredit upon the armed forces.

7. As charged, the elements of Specifications 4,6,8,12, and 16 of Charge II, which alleges a violation of 18 U.S.C. § 641 are (1) that the records described in the specification belonged to the United States government; (2) that the records had a value in excess of \$1,000.00 at the time alleged; (3) that the accused did steal, purloin, or knowingly convert such records to his use or the use of another; (4) that the accused did so knowing the property was not his and with intent to deprive the government of its use or benefit either temporarily or permanently; and (5) that such conduct was prejudicial to good order and discipline in the armed forces and of a nature to discredit upon the armed forces.

8. The elements of a violation of Article 92(1), UCMJ, are (1) that a certain lawful general order or regulation was in effect, (2) that the accused had a duty to obey that order or regulation, and (3) that the accused failed to obey the order or regulation.

9. Defense requests all LIOs that defense agrees are LIO.

#### **LIOs Parties Agree Upon:**

1. **Specifications 2-16 of Charge II: Attempt:** The parties agree that attempt can be a lesser included offense of all of the offenses if raised by the evidence.

2. **Specifications 4,6,8,12, and 16 of Charge II: 18 U.S. C. 641 – property of a value less than \$1,000.00:** The parties agree that this is an LIO.

**3. Specifications 13 and 14 of Charge II: 18 U.S.C. 1030(a)(1): Clause 1 and 2 of Article 134, UCMJ:** The parties agree that this is an LIO.

#### **LIOS in Dispute:**

**1. Specifications 2,3,5,7,9,11, and 15 of Charge II: 18 U.S.C. 793(e): Article 92(1), UCMJ - Violation of Army Regulation (AR) 380-5:** Defense requests. Government opposes on the ground that the elements of Article 92(1), UCMJ are not a subset of 18 U.S.C. 793(e).

**2. Specifications 2,3,5,7,9,11, and 15 of Charge II: 18 U.S.C. 793(e): Clauses 1 and 2 of Article 134, UCMJ:** Government requests. Defense opposes on the ground that the clause 1 and 2 violation must be charged as a violation of a lawful general order.

**3. Specification 1 of Charge II: Article 134, clauses 1 and 2: Article 92(1), UCMJ - Violation of Army Regulation (AR) 380-5:** Defense requests. Government opposes on the ground that the elements of Article 92(1), UCMJ are not subset of the elements of Article 134.

**4. Specifications 4,6,8,12, and 16: 18 U.S.C. 641: Clauses 1 and 2 of Article 134, UCMJ:** Government requests. Defense opposes based on preemption by Article 121, UCMJ.

#### **The Law:**

1. The proper test for determining whether one offense constitutes a lesser included offense of another is the “elements test” from *Schmuck v. United States*, 489 U.S. 705, 716-17 (1989). *United States v. Jones*, 68 M.J. 465, 469-70 (C.A.A.F. 2010). Under the elements test, “one offense is not necessarily included in another unless the elements of the lesser offense are a subset of the elements of the charged offense. Where the lesser offense requires an element not required for the greater offense, no instruction is to be given . . .” *Jones*, 68 M.J. at 469-70 (quoting *Schmuck*, 489 U.S. at 716) (internal quotation marks omitted). The Court must look to Congressional enactments to ascertain the elements of an offense. *Id.* at 471.

2. “[T]he elements test does not require that the two offenses at issue employ identical statutory language. Instead, after applying the normal principles of statutory construction, [the Court] asks whether the elements of the alleged [lesser included offense] are a subset of the elements for the charged offense.” *United States v. Bonner*, 70 M.J. 1, 2 (C.A.A.F. 2011) (citation and internal quotation marks omitted). “The fact that there may be an alternative means of satisfying an element in a lesser offense does not preclude it from being a lesser-included offense.” *United States v. Arriaga*, 70 M.J. 51, 55 (C.A.A.F. 2011). The charged language in the Specifications determines which statutory variables are relevant for purposes of a lesser included offense analysis. *Id.* at 55. “The comparison is drawn between offenses. Since offenses are statutorily defined, that comparison is appropriately conducted by reference to the statutory elements of the offenses in question and not, as the inherent relationship approach would mandate, by reference to conduct proved at trial regardless of the statutory elements of the offenses in question...One element of an offense is not “necessarily included” in another unless the elements of the lesser offense are a subset of the elements of the charged offense.” *U.S. v. Medina*, 66 M.J. 21 (C.A.A.F. 2008).

3. Regarding Article 134, UCMJ, the Manual for Courts-Martial, United States (2012) (M.C.M.) directs that the elements of an assimilated crime or offense not capital are the elements as defined in the applicable law. M.C.M., pt. iv, para. 60(b). If the conduct in question is to be punished under clauses 1 or 2 of Article 134, UCMJ, the elements are twofold: (1) the specific actions the accused did or failed to do, and (2) that the accused's actions or omissions were prejudicial to good order and discipline or of a nature to discredit the armed forces. M.C.M., pt. iv, para. 60(b). Clauses 1, 2, and 3 are alternative theories of prosecution under Article 134. Clauses 1 and 2 are lesser included offenses of clause 3 if the elements of clauses 1 and 2 are plead in the specification. *U.S. v. Medina*, 66 M.J. 21 (C.A.A.F. 2008).

#### Analysis:

#### Specifications 2,3,5,7,9,11, and 15 of Charge II: 18 U.S.C. 793(e): Article 92(1), UCMJ - Violation of Army Regulation (AR) 380-5:

1. The crime or offense not capital that the Government assimilated via clause three of Article 134, UCMJ in Specifications 2, 3, 5, 7, 9, 10, 11, and 15 of Charge II, 18 U.S.C. § 793(e), is a generally applicable, federal criminal statute that is part of the criminal sanctions Congress crafted for espionage. As such, it is not founded upon the existence of a regulation of any of the military services, and Congress did not include a reference to any such authority in establishing the offense found at 18 U.S.C. § 793(e). It is enough that the accused's possession of the specified information was "unauthorized;" the statute does not require more.
2. While a lawful general regulation, such as the one at issue in this case, can serve as the basis for an accused's possession of certain information being unauthorized, the plain language of the statute does not require the existence of any such regulation in order to commit the offense. It is simply irrelevant under the statute what the source of the accused's lack of authority for possessing the information was so long as the accused was, in fact, without that authority. Therefore, it follows that the existence of a lawful general regulation is not necessarily included in a violation of 18 U.S.C. § 793(e). See *Jones*, 68 M.J. at 471.
3. The fact that the regulation in this case can serve as a basis for the lack of authority required in § 793(e) does not alter the analysis. The Specifications in question do not add anything to the statute that would import a requirement for a lawful general regulation into the offense; indeed, they are not permitted to do so for purposes of defining an offense. M.C.M., pt. iv, para. 60(b); see *Jones*, 68 M.J. at 471. The statute also does not include a variable that the Specifications could further refine consistent with *Arriaga*. Instead, § 793(e) specifies the exact conduct required to constitute an offense, and that conduct does not include a failure to obey a lawful general regulation, even though violating a germane lawful general regulation would potentially result in the commission of an offense under § 793(e). To hold otherwise would be to return to the inherent relationship test that the CAAF rejected in *Jones*. The second element of the proposed LIO, Article 92(1) – the accused had a duty to obey the lawful general regulation is not a lesser included element of clauses 1 and 2 of Article 134. Prejudice to good order and discipline and service discrediting conduct does not require that the accused had a duty to obey a lawful general regulation. Based on the elements as charged, it is not impossible to prove 18 U.S.C. 793(e) without also proving a violation of a lawful general order. The Defense's request

for an instruction to the effect that a violation of Article 92, UCMJ, is a lesser included offense of the offenses in Specifications 2, 3, 5, 7, 9, 10, 11, and 15 of Charge II is denied.

**Specification 1 of Charge II: Clause 1 and 2 of Charge II: Clauses 1 and 2 of Article 134, UCMJ:**

Similarly, an Article 92 offense is not a lesser included offense of the Article 134 offense described in Specification 1 of Charge II. The actions alleged in Specification 1 of Charge II do not include a failure to obey a lawful general regulation, and that description defines the scope of the elements for that offense. M.C.M., pt. iv, para. 60(b). While the actions alleged, wrongfully and wantonly publishing government intelligence on the internet, could result in a violation of a lawful general regulation, they do not necessarily include such a violation, and a violation of a lawful general regulation alone would not necessarily constitute an offense as described in Specification 1 of Charge II. See *Jones*, 68 M.J. at 471; cf. *Bonner*, 70 M.J. at 3 (finding that assault consummated by a battery is a lesser included offense of wrongful sexual contact because both offenses require offensive contact). The second element of the proposed LIO, Article 92(1) – the accused had a duty to obey the lawful general regulation is not a lesser included element of clauses 1 and 2 of Article 134. Prejudice to good order and discipline and service discrediting conduct does not require that the accused had a duty to obey a lawful general regulation. Based on the elements as charged, it is not impossible to prove a clause 1 and 2 violation of Article 134 without also proving a violation of a lawful general order. The Defense's request for a lesser included offense instruction for Specification 1 of Charge II is denied.

**Specifications 2,3,5,7,9,11, and 15 of Charge II: 18 U.S.C. 793(e): Clauses 1 and 2 of Article 134, UCMJ:**

1. Under *Medina*, the Court finds that violations of clauses 1 and 2 of Article 134 are lesser included offenses of clause 3 of Article 134 because the clause 1 and 2 elements are plead in the specifications. The Government has not presented the Court with a brief addressing the Defense argument that *U.S. v. Borunda*, 67 M.J. 607 (A.F. Ct. Crim. App. 2009) precludes the clause 1 and 2 LIO, thus the Court declines to instruct on the LIO. The Government may request reconsideration upon in a written filing addressing the issue.

**Specifications 2,3,5,7,9,11, and 15 of Charge II: 18 U.S.C. 793(e): Clauses 1 and 2 of Article 134, UCMJ:**

Under *Medina*, the Court finds that violations of clauses 1 and 2 of Article 134 are lesser included offenses of clause 3 of Article 134 because the clause 1 and 2 elements are plead in the specifications. The Government has not presented the Court with a brief addressing the Defense argument that *U.S. v. Borunda*, 67 M.J. 607 (A.F. Ct. Crim. App. 2009) precludes the clause 1 and 2 LIO, thus the Court declines to instruct on the LIO. The Government may request reconsideration upon in a written filing addressing the issue.

**Specifications 2,3,5,7, 9,10,11, and 15: 18 U.S.C. 641: Clauses 1 and 2 of Article 134, UCMJ:**



Under *Medina*, the Court finds that violations of clauses 1 and 2 of Article 134 are lesser included offenses of clause 3 of Article 134 because the clause 1 and 2 elements are plead in the specifications. The Government has not presented the Court with a brief addressing the Defense argument that Article 121 preempts the clause 1 and 2 LIO, thus the Court declines to instruct on the LIO. The Government may request reconsideration upon in a written filing addressing the issue.

**RULING:** The Motions for LIO instructions by the parties is **GRANTED IN PART** and **DENIED IN PART**.

1. The Court will instruct on attempt as an LIO if raised by the evidence for specifications 2-16 of Charge II:
2. The Court will instruct on property of a value less than \$1,000.00 for specifications 4,6,8,12, and 16 of Charge II.
3. The Court will instruct on clauses 1 and 2, Article 134 as an LIO of specifications 13 and 14 of Charge II.
4. The Court will not instruct on the remaining requested LIOs.

So **ORDERED:** this 8<sup>th</sup> day of June 2012.



DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.


MANNING, Bradley E., PFC  
HHC, U.S. Army Garrison  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

CLASSIFIED INFORMATION  
SEAL ORDER

DATED: 8 June 2012

1. The following exhibit: AE CXL (140) contains classified attorney work product. The exhibit is classified as defined in MRE 505(b) and is classified at the SECRET//NOFORN level. The Government interest in protecting national security is compelling, *Snepp v. U.S.*, 444 U.S. 507, 509, n. 3 (1980). The Court finds that the Government's interest in protecting the national security of the United States and preventing the dissemination of classified information outweighs the public's right of access to this material. This exhibit will be sealed in the record of trial in accordance with RCM 1103A, RCM 1104(b)(1)(D), RCM 701(f), and MRE 505.
2. The Court Security Officer shall cause a proper security classification to be assigned to the record of trial, to each classified exhibit, and to each page of the record of trial in which classified information appears, in accordance with RCM 1103(h). The Court Security Officer will ensure that the sealed exhibits are properly marked, including an annotation on each that the material was sealed by order of the military judge prior to insertion into the original record of trial. Trial counsel will clearly identify in the record of trial where classified exhibits and pages in the record of trial will be maintained.
3. This exhibit contains classified national security information and attorney work product. The classified information shall be handled in a manner consistent with Executive Order 13526. An individual's access to the classified information in this exhibit is subject to the following: having the appropriate security clearance; signing an approved nondisclosure agreement; having a need-to-know the information; and acknowledging the Judicial Protective Order for Classified Information, dated 16 March 2012. Access to the classified information is further restricted by the fact that the classified information is attorney work product.
4. Sealed exhibits will not be opened or examined except for the following:
  - a. Prior to authentication of the record by the military judge, sealed materials may be examined upon order from the military judge based on good cause.
  - b. After authentication and prior to disposition of the record of trial pursuant to RCM 1111, sealed materials may be examined upon order issued from the military judge upon a showing of good cause at a post-trial Article 39(a) session directed by the Convening Authority.
  - c. Reviewing and appellate authorities meeting the criteria in paragraph 3 may examine sealed matters when those authorities determine that such action is reasonably necessary to a proper fulfillment of their responsibilities under the Uniform Code of Military Justice, the Manual for Courts-Martial, governing directives, instructions, regulations, and applicable rules of professional responsibility.
5. No person authorized to examine sealed exhibits shall photocopy, photograph, duplicate, or disclose the contents of the sealed exhibit in the absence from an order by a military judge, the Judge Advocate General or designee, or an appellate court, or other court of competent jurisdiction.

ORDERED, this the 8<sup>th</sup> day of June 2012.

  
DENISE R. LIND  
COL, JA  
Chief Judge, 1st Judicial Circuit

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC  
HHC, U.S. Army Garrison  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

CLASSIFIED INFORMATION  
SEAL ORDER

DATE: 8 June 2012

1. The following exhibit: AE CXLI (141) contains classified information as defined in MRE 505(b). The Government interest in protecting national security is compelling, *Snepp v. U.S.*, 444 U.S. 507, 509, n. 3 (1980). The Court finds that the Government's interest in protecting the national security of the United States and preventing the dissemination of classified information outweighs the public's right of access to this material.

2. The exhibit is classified at the SECRET//NOFORN level. This exhibit will be sealed in the record of trial in accordance with RCM 1103A, RCM 1104(b)(1)(D), and MRE 505.

3. The Court Security Officer shall cause a proper security classification to be assigned to the record of trial, to each classified exhibit, and to each page of the record of trial in which classified information appears, in accordance with RCM 1103(h). The Court Security Officer will ensure that the sealed exhibits are properly marked, including an annotation on each that the material was sealed by order of the military judge prior to insertion into the original record of trial. Trial counsel will clearly identify in the record of trial where classified exhibits and pages in the record of trial will be maintained.

4. This exhibit contains classified national security information. This classified information shall be handled in a manner consistent with Executive Order 13526. An individual's access to the classified information in this exhibit is subject to the following: having the appropriate security clearance; signing an approved nondisclosure agreement; having a need-to-know the information; and acknowledging the Judicial Protective Order for Classified Information, dated 16 March 2012.

5. Sealed exhibits will not be opened or examined except for the following:


a. Prior to authentication of the record by the military judge, sealed materials may be examined upon order from the military judge based on good cause.

b. After authentication and prior to disposition of the record of trial pursuant to RCM 1111, sealed materials may be examined upon order issued from the military judge upon a showing of good cause at a post-trial Article 39(a) session directed by the Convening Authority.

c. Reviewing and appellate authorities meeting the criteria in paragraph 3 may examine sealed matters when those authorities determine that such action is reasonably necessary to a proper fulfillment of their responsibilities under the Uniform Code of Military Justice, the Manual for Courts-Martial, governing directives, instructions, regulations, and applicable rules of professional responsibility.

6. No person authorized to examine sealed exhibits shall photocopy, photograph, duplicate, or disclose the contents of the sealed exhibit in the absence from an order by a military judge, the Judge Advocate General or designee, or an appellate court, or other court of competent jurisdiction.

ORDERED, this the 8<sup>th</sup> day of June 2012.

  
DENISE R. LIND  
COL, JA

Chief Judge, 1st Judicial Circuit

|                   |              |
|-------------------|--------------|
| APPELLATE EXHIBIT | CXCV         |
| Page 1            | of Page(s) 1 |

(145)

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v )

MANNING, Bradley E., PFC )

U.S. Army, xxx-xx- )

Headquarters and Headquarters Company, )

U.S. Army Garrison, Joint Base Myer- )

Henderson Hall, Fort Myer, VA 22211 )

**RULING: DEFENSE MOTION  
TO COMPEL DISCOVERY -  
DAMAGE ASSESSMENTS -  
WIKILEAKS TASK FORCE**

DATED: 22 June 2012

This ruling supplements the 6 June 2012 ruling of the Court regarding the adequacy of the substitute submitted by the Government for the Wiki Leaks task force damage assessment.

The Court reviewed the Government's classified motions for a substitute submitted *ex parte* to the Court. The Court also conducted an *ex parte* review of the original damage assessment and the proposed substitute. In coming to this ruling, the Court has considered the factors requested by the Defense in 1 June 2012 submission.

- a) What is the extent of the redactions/substitutions?
- b) Has the Government narrowly tailored the substitutions to protect a Governmental interest that has been clearly and specifically articulated?
- c) Does the substitution provide the Defense with the ability to follow-up on leads that the original document would have provided?
- d) Do the substitutions accurately capture the information within the original document?
- e) Is the classified evidence necessary to rebut an element of the 22 charged offenses, bearing in mind the Government's very broad reading of many of these offenses?
- f) Does the summary strip away the Defense's ability to accurately portray the nature of the charged leaks?
- g) Do the substitutions prevent the Defense from fully examining witnesses?
- h) Do the substitutions prevent the Defense from exploring all viable avenues for impeachment?
- i) Does the Government intend to use any of the information from the damage assessments? If so, is this information limited to the summarized document provided by the Government? If the information intended to be used by the Government is not limited to the summarized document, does the Defense in fairness need to receive the classified portions of the documents to put the Government's evidence in proper context?
- j) Does the original classified evidence present a more compelling sentencing case than the proposed substitutions by the Government?
- k) Do the proposed substitutions prevent the Defense from learning names of potential witnesses?
- l) Do the substitutions make sense, such that the Defense will be able to understand the context?
- m) Is the original classified evidence necessary to help the Defense in formulating defense strategy and making important litigation decisions in the case?
- n) Is it unfair that the Government had access to the unclassified version of the damage assessment and the Defense did not? Does that provide a tactical advantage to the Government?

On 5 June 2012, the Court made the following ruling with respect to the WikiLeaks Task Force damage assessment: "The Government found no unclassified information in its review of the WikiLeaks Task Force report favorable to the accused and material to guilt or punishment. The Government filed an *ex parte* motion for *in camera* review by the Court IAW MRE 505(g)(2) to determine whether a proposed Government substitution shall be disclosed to the Defense or whether disclosure of the classified information itself is necessary to enable the accused to prepare for trial. The Court has conducted an *in camera* review of the classified information considering the factors requested by the Defense. The Government substitute discloses *Brady* and RCM 701(a)(6) material but not material under RCM 701(a)(2). The Court does not find at this time that the proposed substitute is sufficient. The Court will meet *ex parte* with Government counsel in an area appropriate for review of classified information. A court reporter will transcribe the classified proceedings."

On 7 June 2012, the Court met *ex parte* with the Government in an appropriate place for classified proceedings. The proceeding was recorded. The Court advised the Government to add additional *Brady* material to the substitution. The Government has advised the Court that it has done that.

The Government has advised the Court that nothing in the WikiLeaks Task Force Report will be used by the Government or by any Government witness during any portion of the trial.

The WikiLeaks Task Force Report substitution meets the Government's discovery obligations under *Brady* and RCM 701(a)(6) to disclose evidence tending to reasonably negate the guilt of the accused to an offense charged, reduce the degree of guilt to an offense charged, or reduce the punishment.

The WikiLeaks Task Force Damage Report information not disclosed to the Defense is not material to the preparation of the defense or relevant and necessary for production under RCM 703(f). The Government is ordered that no portion of the WikiLeaks Task Force not disclosed to the Defense will be used by the Government or any Government witness during any portion of the trial. This includes rebuttal and rule of completeness if Defense introduces or references anything in the substitution.

The substitution is sufficient for the Defense to adequately prepare for trial and represents an appropriate balance between the right of the Defense to discovery and the protection of specific national security information.

**RULING:** The Classified motions by the Government to voluntarily provide limited disclosure under MRE 505(g)(2) WikiLeaks Task Force is **GRANTED**.

**Ordered** this 22<sup>nd</sup> day of June 2012.



DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, xxx-xx- )

Headquarters and Headquarters Company, )

U.S. Army Garrison, Joint Base Myer- )

Henderson Hall, Fort Myer, VA 22211 )

**RULING: DEFENSE MOTION  
TO COMPEL DISCOVERY #2**

DATED: 22 June 2012

On 10 May 2012, Defense Moved to Compel Discovery #2 in accordance with (IAW) RCM 701(a)(2), 701(a)(5), 701(a)(6) and 905(b)(4), Article 46, UCMJ, and the Fifth and Sixth Amendments to the Constitution. On 2 June 2012, Defense filed a Motion for Modified Relief. On 7 June 2012, Defense filed an addendum to the Motion to Compel Discovery #2 and on 18 June 2012, Defense filed a second addendum. Government opposes. On 31 May 2012, Government provided the Court Notice of ONCIX damage assessment. On 2 June 2012, Defense responded. After considering the pleadings, evidence presented, and argument of counsel, the Court finds and concludes the following:

**Discovery at Issue:**

1. Full investigative files by the Army Criminal Investigation Division (CID), Defense Intelligence Agency (DIA), Defense Information Systems Agency (DISA), and United States Central Command (CENTCOM) and United States Southern Command (SOUTHCOM) related to PFC Manning, WikiLeaks, and/or the damage occasioned by the alleged leaks IAW RCM 702(a)(2).
2. The Headquarters Department of the Army (HQDA) file related to the 17 April 2012 discovery request IAW RCM 701(a)(2) and RCM 701(a)(6).
3. The entire FBI, Diplomatic Security Service (DSS), Department of State (DOS), Department of Justice (DOJ), Government Agency, Office of the Director of National Intelligence (ODNI), and Office of the National Counterintelligence Executive (ONCIX) files in relation to PFC Manning and/or WikiLeaks (in the alternative produced for *in camera* review to determine whether the evidence is discoverable under RCM 701(a)(2)). If the Court determines that the files are not within the possession, custody, or control of military authorities, Defense requests the Court order production as relevant and necessary under RCM 703(f).
  - a. FBI – (1) FBI investigation. Defense alleges Government has produced heavily redacted files containing only material favorable to the defense and moves for discovery of the entire report of investigation involving PFC Manning or WikiLeaks.

(2) On 31 May 2012, the Government notified Defense that the FBI conducted an Impact Statement for which the Government intends to file an *ex parte* motion under MRE 505(g)(2).

b. DSS – Defense alleges Government has disclosed only items charged in specification 14 of Charge II and moves to compel DSS files dealing with Specifications 12 and 13 of Charge II. Government states it has disclosed the entire file.

c. DOS – Defense moves to compel:

(1) Chief of Mission review of released cables at affected posts concerning their initial assessment as well as their opinion regarding the overall effect that WikiLeaks release could have on relations with the host country, if any. The Chiefs of Mission produced written assessments of the leaked cables based upon their independent review. These written submissions were then used to formulate a portion of the draft damage assessment completed in August of 2011;

(2) WikiLeaks Working Group documents – particularly written Situation Reports approximately twice a week during the groups time period of operation roughly from 28 November 2010 until 17 December 2010.

(3) Mitigation Team documents – particularly written minutes of its meetings and written agendas for it work. Part of the Mitigation Team's efforts concentrated on counterterrorism concerns;

(4) The Persons at Risk Group Information Memorandum for the Secretary of State, matrix to track identified individuals, and formal guidance to all embassies concerning the Department of States' efforts and authorized actions for any identified person at risk;

(5) Information collected by the Director of the Office of Counterintelligence within the Department of State regarding any possible impact from the disclosure of diplomatic cables intended to possibly be used to update the August 2011 draft damage assessment; and

(6) The Department of State's reporting to Congress to include any prepared written statement for Congressional testimony on 7 and 9 December 2010 and Congressional testimony by Ambassador Patrick Kennedy's testimony on 11 March 2011 for members of the House of Representatives and the Senate and the House Permanent Select Committee on Intelligence, and DOS reports to Congress concerning any effect caused by WikiLeaks disclosure and steps undertaken to mitigate them, the 2 briefings for members of the House of Representatives and the Senate in December 2010.

On 8 June 2012, the Court granted the Government's request for 30 days to determine whether the above records exist. On **9 July 2012**, the Government will notify the Court whether such records exist and file a supplemental response to the Defense Motion to Compel Discovery for those records that do exist.

- d. DOJ – documents related to the investigation of PFC Manning and WikiLeaks.
- e. CIA – internal investigation or damage assessment.
- f. ODNI – Internal Review of DOS cables.

g. ONCIX – Documents related to PFC Manning or WikiLeaks. The Government has provided 12 pages of *Brady* material. On 31 May 2012, the Government provided notice to the Court that ONCIX has a draft damage assessment with a coordinated version complete approximately 13 July 2012 and agreed to provide the draft damage assessment to the Court for *in camera* review.

4. Brady material from the Interagency Committee Review, President's Intelligence Advisory Board, House of Representative's Oversight Committee;

5. All evidence intended for use in the Government case-in-chief obtained from DA, DISA, CENTCOM/SOUTHCOM, FBI, DSS, DOS, DOJ, Government Agency, ODNI, and ONCIX.

6. All aggravation evidence the Government intends to introduce in sentencing from DA, DISA, CENTCOM/SOUTHCOM, FBI, DSS, DOS, DOJ, Government Agency, ODNI, and ONCIX.

7. The entire CID, DIA, DISA, and CENTCOM, and SOUTHCOM files related to PFC Manning, WikiLeaks, and/or the damage occasioned by the leaks to include documents, reports, analyses, files, investigations, letters, working papers, and damage assessments. Defense alleges they are material to the preparation of the defense as they will show, what, if any damage was caused by the leaks.

8. Interagency Committee Review: The results of any investigation or review concerning the alleged leaks by Mr. Russell Travers, National Security Staff's Senior Advisor for Information Access and Security Policy. Defense alleges Mr. Travers was asked to lead a comprehensive effort to review the alleged leaks.

9. President's Intelligence Advisory Board: Any report or recommendation concerning the alleged leaks by Chairman Chuck Hagel or any other member of the Intelligence Advisory Board.

10. House Representatives Oversight Committee: The results of any inquiry and testimony taken by House of Representative Oversight Committee led by Representative Darrell Issa. The committee considered the alleged leaks, the actions of Attorney General Eric Holder, and the investigation of PFC Manning.

Defense further moved the Court to require the Government to state with specificity the steps it has taken to comply with RCM 701(a)(6). This issue will be addressed at the Article 39(a) session on 25 June 2012.

#### **The Law:**



1. The Due Process Clause of the Fifth Amendment requires the Government to disclose evidence that is material and favorable to the defense, *Brady v. Maryland*, 373 U.S. 83 (1963).

2. Discovery in the military justice system is governed by Article 46, UCMJ, providing equal opportunity for the parties to obtain witnesses and evidence, and RCM 701, implementing Article 46. These rules provide broader discovery than required by the *Brady* Constitutional standard. *U.S. v. Williams*, 50 M.J. 46 (C.A.A.F. 1999); *U.S. v. Simmons*, 38 M.J. 376 (C.M.A. 1993); *U.S. v. Behenna*, 70 M.J. 521 (Army Ct. Crim. App. 2011); *U.S. v. Trigueros*, 69 M.J. 604 (Army Ct. Crim. App. 2010). RCM 701(a)(6) requires that trial counsel shall, as soon as practicable, disclose to the defense the existence of evidence known to the trial counsel which reasonably tends to negate the guilt of the accused of an offense charged; reduce the degree of guilt of the accused of an offense charged; or reduce the punishment. RCM 701(a)(2) requires the trial counsel, after service of charges, upon request of the defense, to permit the defense to inspect any books, papers, documents, photographs, tangible objects, buildings or places which are within the possession, custody, or control of military authorities and which are material to the preparation of the defense or are intended for use by the trial counsel as evidence in the prosecution case-in-chief at trial or were obtained from or belonged to the accused. The Court of Appeals for the Armed Forces has interpreted RCM 701(a)(2) to require trial counsel to disclose to the defense discoverable information regardless of when the Government intends to use it. *U.S. v. Luke*, 69 M.J. 309 (C.A.A.F. 2011).

3. The Government has a due diligence duty to search for discoverable information both under *Brady* and RCM 701. The scope of the prosecution's requirement to search government files beyond the prosecutor's own files for discovery under RCM 701 and *Brady v. Maryland*, 373 U.S. 83 (1963) is generally limited to: (1) the files of law enforcement authorities that have participated in the investigation of the subject matter of the charged offenses; (2) investigative files in a related case maintained by an entity closely aligned with the prosecution, and (3) other files, as designated in a defense discovery request that involved a specified type of information within a specified entity. The outer parameters are ascertained on a case by case basis. The parameters of the review that must be conducted outside the trial counsel files is dependent on the relationship of the other governmental entity to the prosecution and the nature of the defense discovery request. *U.S. v. Williams*, 50 M.J. 46 (C.A.A.F. 1999) (holding that trial counsel had no duty to review unit disciplinary records for information concerning any investigations or prosecutions of government witnesses, where defense did not specifically request a review of such files. In *Williams*, the defense filed a general request for "any and all investigations or possible prosecutions pending which could be brought against any witness the government intends to call during the trial." *Williams* held this was not a specific request and the trial counsel was not required to review the unit files in which the information was located.) *Williams* went on to state that while the Government has a duty to review prosecution and police files readily available to the prosecution, it is not required to search for "a needle in a haystack".

4. The Government does not have a discovery obligation under RCM 701(a)(2) unless the discovery at issue is within the possession, custody, or control of military authorities, and is material to the preparation of the defense or intended for use by the trial counsel as evidence in the Prosecution case in chief at trial, or was obtained from or belonged to the accused. To the extent relevant files are known to be under the control of another government entity, the

Prosecution must make that fact known to the Defense and engage in good faith efforts to obtain the material. *Williams*, quoting *Simmons*, citing to the Standard 1102.1(a) Commentary, American Bar Association, Criminal Justice Discovery Standards 14 n. 9 (3d ed. 1995).

5. Evidence maintained by other government agencies, whether aligned with the Prosecution or not, are not within the control of military authorities IAW RCM 701(a)(2). (*See analysis* to RCM 701(a)(2) "Except for subsection (c), the rule deals with discovery in terms of disclosure of matters known to or in the possession of a party. Thus, the defense is entitled to disclosure of matters known to the trial counsel or in the possession of military authorities. Except as provided in subsection (c), the defense is not entitled under this rule to disclosure of matters not possessed by military authorities or to have the trial counsel seek out and produce such matters for it.... Subsection (c) may accord the defense the right to have the Government assist the defense to secure evidence or information when not to do so would deny the defense similar access to what the prosecution would have if it were seeking the evidence or the information. See *U.S. v. Killebrew*, 9 MJ 154 (C.M.A. 1980); *Halfacre v. Chambers*, 5 MJ 1099 (C.M.A. 1976).")

6. The burden is on the Defense for production of evidence outside the control of military authorities for discovery under the relevant and necessary standard in RCM 703(f). Evidence that is material to the preparation of the defense under the control of other government agencies can be relevant and necessary for discovery, requiring production of the evidence from the other government entities pursuant to RCM 703(f)(1) and (4)(A).

7. For files pertaining to PFC Manning within the possession, custody, or control of military authorities that the Government is aware of and has searched for *Brady* material, Trial Counsel must turn over to the Defense any information that is obviously material to the preparation of the defense. This does not mean that the Government must search for information material to the preparation of the defense without a specific discovery request. Where a request is necessary, it is required to trigger the trial counsel's duty to disclose as a means of specifying what must be produced. Without such a request a trial counsel might be uncertain as to the extent of the duty to obtain matters not in his/her immediate possession. Any request should state with reasonable specificity what materials are sought. *See analysis* to RCM 701(a).

### **Conclusions of Law:**

1. **Files under the possession, custody, or control of military authorities.** The Government will seek out and identify such files regarding PFC Manning that involve investigation, damage assessment, or mitigation measures. By **20 July 2012** the Government will notify the Court with a status of whether it anticipates any government entity that is the custodian of classified evidence that is the subject of the Defense Motion to Compel will seek limited disclosure IAW MRE 505(g)(2) or claim a privilege IAW MRE 505(c) for the classified information under that agency's control. Also by **25 July 2012**, if the relevant agency claims a privilege under MRE 505(c) and the Government seeks an *in camera* proceeding under MRE 505(i), the Government will move for an *in camera* proceeding IAW MRE 505(i)(2) and (3) and provide notice to the Defense under MRE 505(i)(4)(A). For all such files where a privilege under MRE 505(c) is not claimed, by **3 August 2012** the Government will disclose such files regarding PFC Manning that involve investigation, damage assessment, or mitigation measures to the Defense or, submit them

to the Court for *in camera* review under RCM 701(g) or for limited disclosure under MRE 505(g)(2).

## 2. Aligned Agencies:

**DOJ** – Defense moves to compel documents from DOJ related to the accused, WikiLeaks, and/or alleged leaks because the Government collaborated with federal prosecutors within DOJ during the investigation of the accused. Such files are not discoverable under RCM 701(f). As such, the defense has not shown relevance and necessity for production of DOJ files under RCM 703(f).

**FBI/DSS** – the FBI and DSS are aligned agencies that conducted an investigation of PFC Manning in conjunction with CID. The Government advised the Court it had disclosed the entire DSS investigation to the Defense. The Court finds the Defense has shown that the FBI file (minus grand jury testimony) to the extent relevant to an investigation of PFC Manning, is material to the preparation of the Defense to the extent that it is relevant and necessary for production under RCM 703(f). The Court will review the FBI Impact Statement *in camera* to determine whether it is material to the preparation of the defense to the extent relevant and necessary to require production for disclosure. The Government will **immediately** begin the process of producing the FBI investigative file and impact statement IAW RCM 703(f)(4)(A). By **25 July 2012** the Government will notify the Court with a status of whether it anticipates any government entity that is the custodian of classified evidence that is the subject of the Defense Motion to Compel will seek limited disclosure IAW MRE 505(g)(2) or claim a privilege IAW MRE 505(c) for the classified information under that agency's control. Also by **25 July 2012**, if the relevant Government agency claims a privilege under MRE 505(c) and the Government seeks an *in camera* proceeding under MRE 505(i), the Government will move for an *in camera* proceeding IAW MRE 505(i)(2) and (3) and provide notice to the Defense under MRE 505(i)(4)(A). For all such files where a privilege under MRE 505(c) is not claimed, by **3 August 2012** the Government will disclose such files regarding PFC Manning that involve investigation, damage assessment, or mitigation measures to the Defense or, submit them to the Court for *in camera* review under RCM 701(g) or for limited disclosure under MRE 505(g)(2).

**ODNI/ONCIX** – NLT **3 August 2012**, The Government will provide the Court with the damage assessment for *in camera* review. The Government has stated in its briefs that ONCIX is not an aligned agency but has not asked the Court to reconsider the portion of the 23 March 2012 ruling stating that it was.

**CIA** – The Court has conducted an *in camera* review of the WikiLeaks Task Force Damage Assessment and the proposed Government substitute under IAW MRE 505(g)(2). The Court's ruling with respect to this damage assessment is issued as a separate Appellate Exhibit.

## 3. Other.

**DOS** – The Court granted the Government's request for 30 days to respond to the Defense Motion to Compel DOS documents. On **9 July 2012** the Government will identify which files exist and provide its position to the Court IAW the Court's order of 8 June 2012.

**17 April 2012 HQDA file** – The Government alleges there is no “file”. What, if any, file exists will be addressed at the Article 39(a) session on 25 June 2012.

**Government Evidence in Merits/Sentencing – NLT 3 August 2012**, the Government shall disclose evidence it will introduce on the merits and during sentencing.

**Interagency Committee Review, President's Intelligence Advisory Board, and House of Representative Oversight Committee.** The Defense moves to compel the Government to conduct *Brady* searches of the files of these entities. These are non-aligned entities who have had no interaction or involvement with the Prosecution or the Criminal Investigation in this case. Their files are not readily available to the Prosecution. The Prosecution has had no access to these entities or their files. Although the Defense has made a specific request that the Court compel the Government to conduct a *Brady* search of these files, the Court finds that the files of these entities are too attenuated and beyond the outer parameters of the core files the Prosecution must search for *Brady*. The Government advised the Court that it had an ethical obligation to search the President's Intelligence Advisory Board for *Brady* material because it had reason to believe the files contained *Brady* material. As such, the Government will conduct a *Brady* search of the President's Intelligence Advisory Board files. The Court does not compel the Prosecution to search the files of the Interagency Committee Review or the House of Representative Oversight Committee.

**RULING:** The Defense Motion to Compel Discovery #2 is **Granted** in part as set forth above.

So **ORDERED:** this 22nd day of June 2012.



DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**Prosecution Request  
for Leave to File  
Motions in Limine After  
Elements are Defined**

**15 June 2012**

1. The United States requests leave of the Court to file its motions in limine, including its motions filed under Military Rule of Evidence (MRE) 404(b), until the Court rules on the proposed elements and definitions for the charged misconduct as defined in the Proposed Members Instructions for all Charged Offenses.<sup>1</sup> The current scheduling order would make the filing date of these motions 3 August 2012.
2. In its motions in limine, the United States is arguing what information should be admissible and should be precluded based on its relevancy to the charged offenses and permissible defenses. If the Court does not rule in favor of the Prosecution's Proposed Members Instructions for all Charged Offenses, portions of the prosecution's argument and the defense's responses will likely change.
3. The prosecution's request will not necessitate any delay in the proceedings; it simply moves the motions in limine from being considered at the 16-20 July 2012 session to the following session. As such, there is no prejudice to the defense.
4. In the alternative, on 22 June 2012 the United States will file its motions based on its proposed elements and definitions, and then file a supplemental motion if any of the elements or definitions are substantially different.



ASHDEN FEIN  
MAJ, JA  
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 15 June 2012.



ASHDEN FEIN  
MAJ, JA  
Trial Counsel

<sup>1</sup> The United States enumerated the other crimes, wrongs, or acts on which it intended to present evidence to the defense on 6 April 2012.

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC  
U.S. Army, xxx-xx-  
Headquarters and Headquarters Company,  
U.S. Army Garrison, Joint Base Myer-  
Henderson Hall, Fort Myer, VA 22211

ORDER: DUE DILIGENCE/  
WITNESSES/GOVERNMENT  
MOTIONS IN LIMINE

DATED: 19 June 2012

Having considered the Defense Proposed Court Calendar submitted via email to the Court on 11 June 2012, the Addendum #2 to Defense Motion to Compel Discovery #2: Request for Witnesses submitted via email to the Court on 18 June 2012, the Government's Prosecution Request to File Motions in Limine After Elements are Defined, submitted via email to the Court on 15 June 2012, and the emails submitted by the parties on 14 and 18 June 2012, the Court orders as follows:

1. Government will file its Due Diligence Response by 20 June 2012. If Defense files a reply, it is due on 22 June 2012. The targeted briefs regarding the Government Motion to Preclude Actual Harm or Damage evidence on the merits and the Government's proposed case calendar are due on 21 June 2012.
2. Defense motion requesting that the Government produce witnesses from the National Counterintelligence Executive (ONCIX), the Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS) for the Article 39(a) session on 25 June 2012 is untimely. These witnesses are not relevant and necessary for the Court to rule on the Due Diligence Motion. The Defense Motion to produce witnesses is **Denied**.
3. Defense does not object to the Government Motion for Leave to File its Motions in Limine, including MRE 404(b) until after the Court rules on the proposed Instructions for the charged offenses. The Government motion is **Granted**. The Government Motions in Limine are continued from the July Article 39(a) term to the August Article 39(a) term.

So **ORDERED**: this 19<sup>th</sup> day of June 2012.



DENISE R. LIND  
COL., JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

DEFENSE PROPOSED CASE  
MANAGEMENT ORDER

11 June 2012

The Court is currently scheduling Article 39(a) sessions with the following default schedule at the request of the parties: two weeks for parties to file motions; two weeks for parties to file responses; five days for parties to file replies; and one week for the Court to review all pleadings before the start of the motions hearing. The Court is also scheduling a separate Article 39(a) session to discuss any substantive issues that may arise between the motion sessions.

a. Phase 1. Immediate Action (21 February 2012 - 16 March 2012)

b. Phase 2(a). Legal Motions excluding Evidentiary Issues (29 March 2012 - 26 April 2012)

c. Phase 2(b). Legal Motions (10 May 2012 - 8 June 2012)

d. 39(a) Session (25 June 2012)

(1) **Due Diligence Motion**

- (A) Filing: 18 June 2012
- (B) Response: 21 June 2012
- (C) Reply: N/A
- (D) Article 39(a): 25 June 2012

(2) **Targeted Briefs on Absence of Harm**

- (A) Filing: 21 June 2012
- (B) Response: N/A
- (C) Reply: N/A
- (D) Article 39(a): 25 June 2012

e. Phase 3a. Evidentiary Issues (22 June 2012 - 20 July 2012)

- (A) Filing: 22 June 2012
- (B) Response: 6 July 2012
- (C) Reply: 11 July 2012
- (D) Article 39(a): 16-20 July 2012

- (1) **Witness List - Government**  
(A) Filing: 22 June 2012  
(B) Response: N/A
- (2) **Proposed Members Instructions for all Charged Offenses and LIOs**
- (3) **Government Pre-Authenticate/Pre-Admit Evidence**
- (4) **Defense Motion to Dismiss All Charged Offenses under 18 U.S.C. 1030(a)(1) #2**
- (5) **Government Motion in Limine (likely admissibility of MRE 404(b) information)**
- (6) **Updated Proposed Case Calendar**  
(A) Filing: 6 July 2012  
(B) Response: 11 July 2012
- (7) **Proposed Questionnaires**  
(A) Filing: 6 July 2012  
(B) Response: 11 July 2012  
(C) Article 39(a): 16-20 July 2012

f. **39(a) Session (13 August 2012)**

g. **Phase 3b. Evidentiary Issues (3 August 2012 – 31 August 2012)**

- (1) **Defense Article 13 Motion**  
(A) Filing: 27 July 2012<sup>1</sup>  
(B) Response: 17 August 2012  
(C) Reply: 24 August 2012  
(D) Article 39(a): 29-31 August 2012

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

---

<sup>1</sup> The filing date is a week earlier for the Defense in order to provide the United States with one additional week for its response.



UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Prosecution Proposed  
Case Calendar  
Update

21 June 2012

1. The proposed calendar is based upon the same assumptions listed in the Prosecution Proposed Case Calendar (AE I) and all Prosecution Proposed Case Calendar Updates and Supplements (including AE XX, XLV, XLVI, and CXIII). To the extent these assumptions prove to be incorrect or too ambitious, the schedule will be correspondingly longer.

2. Prosecution Proposed Calendar:

a. Immediate Action (21 February 2012 - 16 March 2012)

b. Legal Motions, excluding Evidentiary Issues (29 March 2012 - 26 April 2012)

c. Legal Motions (10 May 2012 - 8 June 2012)

d. Pretrial Motions (2 June 2012 - 25 June 2012)

(A) Article 39(a): 25 June 2012

(1) **Supplemental Filings on Actual Damage on the Merits**

(A) Filings: 21 June 2012

(2) **Due Diligence Motion**

(A) Filing: 2 June 2012

(B) Response: 20 June 2012

(C) Reply: 22 June 2012

(3) **Updated Proposed Case Calendar**

(A) Filing: 21 June 2012

e. Pretrial Motions (7 June 2012 - 20 July 2012)

(A) Filing: 22 June 2012

(B) Response: 6 July 2012

(C) Reply: 11 July 2012

(D) Article 39(a): 18-20 July 2012

**(1) Defense Motion to Compel Discovery #2 (Department of State Material)<sup>1</sup>**

- (A) Filing: 7 June 2012
- (B) Response: 8 July 2012
- (C) Reply: 11 July 2012
- (D) Article 39(a): 18-20 July 2012

**(2) Government Initial Witness List**

- (A) Filing: 22 June 2012

**(3) Proposed Members Instructions for All Charged Offenses**

**(4) Witness Lists for Article 13<sup>2</sup>**

- (A) Defense Witness Lists: 6 July 2012
- (B) Government Objections (if any): 10 July 2012
- (C) Defense Motion to Compel (if any): 13 July 2012
- (D) Article 39(a): 18-20 July 2012

**(5) Preliminary Determinations on Admissibility<sup>3</sup>**

**(6) Defense Motion to Dismiss All Charged Offenses under 18 U.S.C. 1030(a)(1) #2**

**(7) Defense Motion to Compel Discovery #3<sup>4</sup> (if any)**

**(8) Maximum Punishment for Lesser Included Offenses**

**(9) Proposed Questionnaires**

- (A) Filing: Parties will confer and arrive at a questionnaire before the Article 39(a) at 16-20 July 2012 session
- (B) Article 39(a): Disagreements will be addressed at Article 39(a) at 16-20 July 2012 session
- (C) Questionnaires to Detailed Members and Alternates: 24 July 2012
- (D) Suspense for Detailed Members and Alternates to Respond to Questionnaires: 3 August 2012

---

<sup>1</sup> See Appellate Exhibit CXLII.

<sup>2</sup> The parties will confer on witness lists before the 25 June 2012 Article 39(a) to determine if the witness list litigation is necessary.

<sup>3</sup> The prosecution plans on moving to pre-admit evidence that has MRE 902(11) attestations.

<sup>4</sup> If any of the information is determined discoverable, then additional time will be needed to determine what, if any, discovery exists. If discovery does exist and if it is classified, the organization owning the information will need time to either disclose, give limited disclosure, or claim a privilege. The Court may have to review additional information and the prosecution may need to request an *in camera* proceeding. The potential *in camera* proceeding is included in this proposal.

**f. Pretrial Motions (27 July 2012 – 8 August 2012)**

- (A) Filing: 27 July 2012
- (B) Response: 3 August 2012
- (C) Article 39(a): 8 August 2012

**(1) Updated Proposed Case Calendar**

**g. Pretrial Motions (27 July 2012 – 31 August 2012)**

- (A) Filing: 3 August 2012
- (B) Response: 17 August 2012
- (C) Reply: 22 August 2012
- (D) Article 39(a): 29-31 August 2012

**(1) Article 13**

- (A) Filing: 27 July 2012<sup>5</sup>

**(2) Motions in *Limine***

**(3) Motions to Suppress**

**(4) Disclosure of Any Remaining Unclassified Results of Information from Motions to Compel Discovery #2 and #3**

- (A) Filing: 3 August 2012

**(5) Disclosure under RCM 701(g)(2) or MRE 505(g)(2) of All Information (Unclassified and Classified) to the Court in Response to Court Rulings for Motions to Compel Discovery #2 and #3 or Notification to the Court of Privilege under MRE 505(c)**

- (A) Filing: 3 August 2012

**(6) Government Filing for *In Camera* Proceeding IAW MRE 505(i) with Notice to Defense (if Privilege is Claimed) in Response to the Court Rulings for Motions to Compel #2 and #3 (if any)**

- (A) Filing: 3 August 2012

**(7) Disclosure of All Remaining Unclassified or Classified (under MRE 505(g)(1)) Brady Material and Disclosure under MRE 701(g)(2) or MRE 505(g)(2) of All Remaining Classified Brady Material<sup>6</sup>**

- (A) Filing: 3 August 2012

---

<sup>5</sup> The defense agreed to the filing date of one week earlier to give the United States the necessary time to respond.

<sup>6</sup> This production is for all material that is not subject to Motions to Compel Discovery or Production. This review will require the same additional time of no more than fifteen duty days. If the Court rules that any of the proposed summaries under MRE 505(g)(2) are not acceptable, the prosecution will need additional time to obtain approval for a different substitution.

**h. Pretrial Motions (31 August 2012 – 19 September 2012)**

- (A) Filing: 7 September 2012
- (B) Response: 14 September 2012
- (C) Article 39(a): 19 September 2012

**(1) Updated Proposed Case Calendar**

**i. Pretrial Motions (7 September 2012 – 12 October 2012)**

- (A) Filing: 14 September 2012
- (B) Response: 28 September 2012
- (C) Reply: 3 October 2012
- (D) Article 39(a): 10-12 October 2012

**(1) Speedy Trial, including Article 10**

- (A) Date: 7 September 2012<sup>7</sup>

**(2) Witness List (Defense and Supplemental Government)**

- (A) Filing: 14 September 2012
- (B) Government Objection to Defense Witnesses: 21 September 2012
- (C) Motion to Compel Production: 28 September 2012
- (D) Response: 3 October 2012
- (E) Article 39(a): 10-12 October 2012

**(3) Defense Notice of its Intent to Offer the Defense of Alibi, Innocent Ingestion, or Lack of Mental Responsibility IAW RCM 701(b)(2)**

**(4) Defense Notice of Intent to Disclose Classified Information under MRE 505(h)(1)**

**(5) Defense Production of Government Reciprocal Discovery Request**

- (A) Date: 14 September 2012

**(6) Government Motion to Compel Discovery (if any)**

- (A) Filing: 28 September 2012
- (B) Response: 3 October 2012
- (C) Article 39(a): 10-12 October 2012

**(7) Defense Notice of Accused's Forum Selection and Notice of Pleas in Writing<sup>8</sup>**

---

<sup>7</sup> The defense agreed to the filing date of one week earlier to give the United States the necessary time to respond.

<sup>8</sup> If the accused selects a panel, the United States proposes the panel be notified no less than sixty days prior to trial, in order to coordinate for extended special duty and travel.

**(8) Motions *in Limine* (Supplemental, Including any Classified Information)**

**j. Pretrial Motions (19 October 2012 – 31 October 2012)**

- (A) Filing: 19 October 2012
- (B) Response: 26 October 2012
- (C) Article 39(a): 31 October 2012

**(1) Updated Proposed Case Calendar**

**(2) Production of Compelled Discovery for Government Motion to Compel Discovery**

- (A) Date: 19 October 2012

**k. Pretrial Motions (26 October 2012 – 30 November 2012)**

- (A) Filing: 26 October 2012
- (B) Response: 9 November 2012
- (C) Reply: 14 November 2012
- (D) Article 39(a): 28-30 November 2012<sup>9</sup>

**(1) Pre-Qualify Government Experts**

**(2) Requests for Judicial Notice**

**(3) Supplemental Government Witness List<sup>10</sup>**

**l. Pretrial Motions (7 December 2012 – 20 December 2012)**

- (A) Filing: 7 December 2012
- (B) Response: 14 December 2012
- (C) Article 39(a): 19-20 December 2012

**(1) Litigation Concerning MRE 505(h) and MRE 505(i)<sup>11</sup>**

- (A) Filing: 14 November 2012
- (B) Response: 27 November 2012<sup>12</sup>

---

<sup>9</sup> The United States scheduled the hearing one week later due to the Thanksgiving holiday.

<sup>10</sup> The United States will submit a supplemental witness list based solely on any rulings from the government motion to compel discovery ruling and any disclosures by the defense after the 14 September 2012 witness list due date.

<sup>11</sup> This includes *in camera* proceedings for Defense Notice to Disclose Classified Information and/or the Government's Invocation of the Privilege for Merits and Sentencing Information. The United States estimates that any Court order to disclose classified information will likely require coordination with multiple federal organizations and roughly estimates forty-five to sixty days to aggressively coordinate a response across all equity holders.

<sup>12</sup> The adjusted date gives the Court additional time to review any discoverable material and was agreed to by the defense. The Government estimates the review will take no more than fifteen duty days to complete.

(C) Article 39(a): 19 December 2012

**(2) Updated Proposed Case Calendar (if necessary)**

**m. Pretrial Motions (14 December 2012 – 11 January 2013)**<sup>13</sup>

(A) Filing: 14 December 2012

(B) Response: 28 December 2012

(C) Reply: 2 January 2013

(D) Article 39(a): 9-11 January 2013

**(1) Any Additional Motion that does not have an Identified Deadline**

**(2) Grunden Hearing for All Classified Information**

**(3) Voir Dire Questions, Flyer, Findings/Sentence Worksheet, All CMCOs**

(A) Filing for Court Review: 2 January 2013

(B) Article 39(a): 9-11 January 2013

**n. Trial by Members (18 January 2013 – 8 February 2013)**

(1) Voir Dire: 18 January 2013

(2) Trial: 21 January 2013-8 February 2013



ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel

<sup>13</sup> There have been numerous unplanned motions submitted throughout the pre-trial process. The prosecution, therefore, anticipates that several pretrial motions will be filed under the "Any Additional Motion" timeframe.

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES )

v. )

MANNING, Bradley E., PFC )

U.S. Army, xxx-xx- )

Headquarters and Headquarters Company, U.S. )

Army Garrison, Joint Base Myer-Henderson Hall, )

Fort Myer, VA 22211 )

**ADDENDUM #2 TO DEFENSE  
MOTION TO COMPEL  
DISCOVERY #2: REQUEST  
FOR WITNESSES**

18 June 2012

RELIEF SOUGHT

1. The Defense reiterates its request for relief in Appellate Exhibit CI. Specifically, the Defense requests the Court to suspend these proceedings and order the Government to state with specificity the steps it has taken to comply with its discovery obligations under R.C.M. 701(a)(2); 701(a)(6), and 905(b)(4), Manual for Courts-Martial (M.C.M.). The Defense also requests that this Court order the Government to produce a witness from the Office of the National Counterintelligence Executive (ONCIX), the Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS) who can testify regarding the representations made to the trial counsel concerning any damage assessment/impact statement being produced by ONCIX, FBI and DHS.

EVIDENCE

2. The Defense requests that this Court order the Government to produce the following witnesses:

a) A witness from the Office of the National Counterintelligence Executive (ONCIX) who can testify to:

- i) the representation made to trial counsel in February 2012;
- ii) the representation made to trial counsel in March 2012;
- iii) what ONCIX had by way of a damage assessment in February and March 2012; and
- iv) the contents of the 18 May meeting with ODNI.

b) A witness from the Federal Bureau of Investigation (FBI) who can testify as to when the FBI had something by way of a damage assessment/impact statement, and when trial counsel had knowledge of this fact.

c) A witness from the Department of Homeland Security (DHS) who can testify as to when the DHS had something by way of a damage assessment, and when trial counsel had knowledge of this fact.

### FACTS

3. On 31 May 2012, the Government provided notice to the Court and the Defense that ONCIX had a draft damage assessment. Along with the Government's notice, it provided a copy of its 24 May 2012 letter to ONCIX and the reply by ONCIX on 30 May 2012. Appellate Exhibit CXIX. On that same day, the Government notified the Court and Defense that the FBI had conducted an impact statement. Appellate Exhibit C.

4. On 2 June 2012, the Defense filed its Response to the Government's notice of the ONCIX damage assessment in Appellate Exhibit 120, and also addressed Government's statement that it had "discovered" an FBI impact statement in Appellate Exhibit CI.

5. On 6 June 2012, the Court orally required the Government to account for its efforts regarding each of the identified agencies within the Defense's Motion to Compel Discovery #2 during an Article 39(a) session. The Court discussed FBI and ONCIX with the Government.

6. With regards to the FBI, the Government did not indicate when it learned of the FBI impact statement. When the Court asked the Government if it was prepared to discuss when it first learned of the FBI impact statement, the Government balked. Instead, of responding to the Court's question, the Government only told the Court of the date that it first obtained approval to provide the FBI impact statement to the Defense under M.R.E. 505(g)(2). The Government believed the date it received approval from the FBI to turn over the impact statement was on 18 May 2012. Instead of immediately alerting the Court and the Defense, the Government buried the existence of the FBI impact statement in its 31 May 2012 filing which was intended to respond to the Defense's Supplement to the Motion to Compel Discovery #2. Appellate Exhibit C, p. 4.

7. With regards to the ONCIX damage assessment, the Court and the Government engaged in the following colloquy:

COURT: Why did you tell me back on the 21<sup>st</sup> of March that NCIX or ONCIX had no damage assessment? Those were not the exact words you used but go ahead and tell me-

MAJ Fein: Correct your Honor. Your Honor, frankly. Because we do not have access. Or even knowledge, absent us asking a question and receiving it to these files because of the nature of this type of assessment. We ask the questions based off of the Defense's discovery requests. Specifically your Honor, if it may please the Court to kind of lay out a time line. This is, this is somewhat reflected in the Defense's motion from Saturday. But, 16 February 2012 was the Defense's motion to compel discovery, their first motion. On 28 February 2012 was the first 802 conference. After the 16 February 2012 motion to compel, we approached at some point, I don't have that date, NCIX through ODNI and said "we are required to produce the following, here is an example of what it is. What do



you have?" And then their response of course given was the department of, "ONCIX has not completed a damage assessment – to date they have not produced any interim or final damage assessment in this matter." That is what they gave us and told us.

COURT: Did they do that orally or in writing?

MAJ Fein: Orally your Honor. And so, by us writing that down, and inquiring "is this all you have, is this what it is?" And this is the response we received. That is ultimately what we – fast forward, at the motions hearing, on the record, both at the 802 conference after the motions hearing, and on the email inquiry on 21 March, when asked. As you will notice from the Court's motion to compel discovery dated 23 March 2012, the Court documented the email questions and those email questions were "does the damage assessment essentially exist with ODNI, or excuse me with ONCIX." And we responded in an email "ONCIX has not produce any interim or final damage assessments in this matter." We asked them the questions. We don't have any other access to their files. They answered it. So, at that point we relayed that to the Court, we relayed it to the Defense and the Court ruled. Then –

COURT: At that time, is it the Government's belief that they didn't have anything?

MAJ Fein: Correct your Honor. It is our belief, at that point, that they were compiling these other assessments we knew about because we started reaching out once they told us about it – to go get those. But, that they had no other documentation that would be subject to discovery – based off this response. So, yes we did know that their individual organizations were submitting theirs, and that is why we went out to those independent organizations to get them approval and disclose them.

COURT: MAJ Fein, you understand that the purpose of the questions from the Court was to discover what's out there?

MAJ Fein: Yes, your Honor. And the prosecution did exactly that, your Honor. Even after the email from the Court, the prosecution reached out to ODNI and NCIX to ask the question again and this was the response we received. And it goes back to the military authorities line of, line of inquiry. That a military prosecutor, even a Department of Justice prosecutor, doesn't necessarily have access to walk into any government building and search the files. We asked questions, we give them the relevant cases, the case law, we show them the discovery requests and any other orders. And then they give us the answer. Or give us access and we go search them for the answer. And in this case, they gave us the answer. We relayed that to the Court.

*-Later after the Defense indicated that the Government had to have known that ONCIX was creating a damage assessment-*

COURT: So the Government's position if I am understanding it then, is that you saw a distinction between the Department of State – which you told me the Department of State has not completed a damage assessment; and – I guess what is the difference between

what the Department of State's position was at that time and what ONCIX's was at that time?

MAJ Fein: Your Honor, to be honest, the Government does not necessarily know. We asked the questions and this is what we are given and what we relayed to the Court...

8. On 8 June 2012, the Government provided Defense with oral notification of the existence of the DHS damage assessment. The Government has not yet provided notice to the Court. The Government did not indicate when it first learned of the damage assessment or why it had not provided notice to the Court or the Defense of its existence prior to this date. The Government simply stated that 8 June 2012 was the first time that it was authorized to provide notice of the damage assessment to the Defense.

9. On 15 June 2012, the Defense requested the Government to indicate when it intended to file its submission regarding the due diligence accounting for which it requested a two week extension. Within minutes, the Government responded that it did not intend to file until 21 June 2012. The Defense immediately replied, and informed the Government that a filing on 21 June 2012 would not provide the Defense with an opportunity to respond or the Court with an adequate amount of time to consider the filings prior to the Article 39(a). *See* Attachment. The Government did not respond.

#### ARGUMENT

10. The Government has represented that it has simply relayed to the Court what it was told from ONCIX. Unfortunately, the timeline provided by the Government and the representations by the Government during oral argument and in Court filings regarding what it knew and when concerning ONCIX do not mesh. The Government would have us believe that, while it knew that ONCIX was compiling a damage assessment starting in October 2010, it blindly relied on an oral assertion from some person at ONCIX in February 2012 that "ONCIX has not produced any interim or final damage assessments in this matter." Just to double check, apparently, the Government called up ONCIX a few weeks later in March 2012 and said something to the effect, "Are you sure you don't have anything?" And again, some person at ONCIX once again said "ONCIX has not produced any interim or final damage assessments in this matter." And the Government once again blindly took that person's word for it. And apparently, a mere two months later, ONCIX went from not having anything worth disclosing to the Court to having a discoverable draft. So, the Government would have us believe that from October 2010 until March 2012 (almost a year and a half), ONCIX did not have anything that would be considered a draft or an interim report; but then a mere two months later, it would have a draft that was nearing a final report. And, of course, regardless of what ONCIX told the Government about the status of its draft (or non-draft), none of this excuses the fact that the Government did not tell the Court or the Defense that ONCIX had something "in the works." Something is not right with the Government's account of the ONCIX story – and a witness from ONCIX should testify so as to set the record straight.

11. The Government has also represented to the Court that it recently "discovered that the FBI conducted an impact statement, *outside of the FBI law enforcement file*, for which the prosecution intends to file an ex parte motion under MRE 505(g)(2)." Appellate Exhibit C at p. 4. Yet, in its 22 March 2012 statement to the Court, the Government stated "the United States is concurrently working with other Federal Organizations which we have a good faith basis to believe may possess damage assessments or *impact statements*...." See Prosecution's Response to Court's Email Questions (22 March 2012). The term "impact statements" within this document is clearly referencing the FBI impact statement.<sup>1</sup> The Government undoubtedly knew of the FBI impact statement prior to its 22 March 2012 disclosure to the Court. The Government, however, failed to notify the Court on that date of the FBI impact statement. The Government also failed to notify the Court of the FBI impact statement on 20 April 2012 when it represented what the FBI had in its possession and that "the United States anticipates that the FBI is the only government entity that is a custodian of classified forensic results or investigative files relevant to this case that will seek limited disclosure IAW MRE 505(g)(2)." Appellate Exhibit LVI.

12. Based upon the Governments responses, either the respective agencies are being less than truthful with the Government, or the Government is being less than truthful with the Court. This Court should require the Government to produce a witness from ONCIX, FBI, and DHS who can testify regarding the representations by the respective agencies to the trial counsel. The Court should not permit the misrepresentations by either various agencies or the trial counsel to frustrate discovery in this case.

#### CONCLUSION

13. The Defense requests that this Court order the Government to produce a witness from ONCIX, FBI, and DHS who can testify regarding the representations made to the trial counsel concerning any damage assessment/impact statement.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

---

<sup>1</sup> Though, of course, the Court and the Defense did not know this at the time due to our belief that the FBI did not have any damage assessment.

# ATTACHMENT

## David Coombs

---

**From:** David Coombs <coombs@armycourtartialdefense.com>  
**Sent:** Friday, June 15, 2012 5:44 PM  
**To:** 'Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA'; 'Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA'; 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; 'Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA'; Alexander.VonElten@jfhqncr.northcom.mil  
**Cc:** Hurley, Thomas F MAJ USARMY (US) (thomas.f.hurley4.mil@mail.mil); 'Tooman, Joshua J CPT USARMY (US)'  
**Subject:** Update

Ashden,

Please provide feedback on the following:

- 1) Article 39(a): Please have PFC Manning at the courthouse at 0900 on 25 June. I want to be able to go over some documentation with him.
- 2) Case Calendar: Are you planning on submitting a case calendar or commenting on the calendar the Defense submitted on Monday? If so, when?
- 3) Motions: When is the Government filing its Due Diligence response motion and its targeted brief on damage?
- 4) Sanitized Versions: Do you have an update on being able to provide unclassified versions of the various damage assessments?
- 5) Department of Homeland Security Damage Assessment: Have you sent this to the NWC?
- 6) Redactions: Are you still planning on submitting your response tomorrow – or did you mean today?
- 7) Replacement for Santiago: TDS does not have the ability to provide a replacement warrant officer for CW2 Santiago. Can the Government provide a suitable replacement?

Best,  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
[coombs@armycourtartialdefense.com](mailto:coombs@armycourtartialdefense.com)  
[www.armycourtartialdefense.com](http://www.armycourtartialdefense.com)

## David Coombs

---

**From:** Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA <Ashden.Fein@jfhqncr.northcom.mil>  
**Sent:** Friday, June 15, 2012 6:12 PM  
**To:** David Coombs  
**Cc:** Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US); Santiago, Melissa S CW2 USARMY (US); Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA; Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA  
**Subject:** Update

David,

Below is an update on your questions and other issues.

1. Article 39(a). We will have PFC Manning at the courthouse at 0900 on 25 June.
2. Case Calendar. We intend to submit a case calendar update on Thursday with our other filings.
3. Motions. We intend to submit our two filings on Thursday, as per our discussion last week.
4. Sanitized Versions of Damage Assessments. We have provided the defense all the damage/impact assessments that exist within each agency or organization. The government did not produce unclassified versions of the damage assessments for the ones that are classified and which have been produced; therefore, there are no unclassified or sanitized versions to provide.
5. Department of Homeland Security Damage Assessment. As stated on Friday, we sent the request earlier this week and NWC received it on Wednesday. Additionally, CW2 Santiago signed for a copy on Wednesday. I apologize for not notifying you sooner of the tracking number or confirmed delivery.
6. Redactions. We will file with the Court tonight and we do not intend to request protective orders.
7. Replacement for Santiago. As previously stated, MDW was informed that the Chief, TDS coordinated directly or indirectly with you for personnel issues concerning the defense. After confirming with the Chief Warrant Officer of the Corps, it is our understanding that all future personnel requests for any personnel, will be handled through TDS channels. Please address any personnel issues through the military defense counsel and their RDC.
8. Defense Expert Request. We have not resolved the issue of the defense requesting that your experts have their time dedicated primarily to the defense. Does the defense intend to request this? Without a request which outlines the anticipated scope of their additional duties (which is already written in your proposed memo) and an estimate of the total time you anticipate you will need their services, we cannot go to their leadership and the convening authority for approval. The leaders must know how much time you anticipate will be needed and to what extent, so they can make informed decisions. Once we receive a request, we will immediately take the request to your experts' leadership and the convening authority for action.

Have a good weekend.

## David Coombs

---

**From:** David Coombs <coombs@armycourt martialdefense.com>  
**Sent:** Friday, June 15, 2012 6:31 PM  
**To:** 'Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA'  
**Cc:** 'Hurley, Thomas F MAJ USARMY (US)'; 'Tooman, Joshua J CPT USARMY (US)'; 'Santiago, Melissa S CW2 USARMY (US)'; 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; 'Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA'; 'Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA'; 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; 'Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA'  
**Subject:** RE: Update

Ashden,

- 1) Thank you.
- 2) Why do you feel that Thursday is the agreed upon date for the case calendar?
- 3) Same as #2 - I don't recall any discussion that Thursday was the timeline for this issue. Not only would this give no time for the Defense to reply, it also does not provide the Court with time to consider the motions prior to the Article 39(a).
- 4) The Defense is requesting that the various agencies produce an unclassified version of their damage assessments. According to the defense security experts, this is not an unusual request.
- 5) Not a problem. Thank you.
- 6) Thank you.
- 7) As stated, TDS cannot provide a replacement warrant officer. I am requesting that the Government provide a replacement for CW2 Santiago. Please inform me if the Government's position is that it will not do so.
- 8) The Defense does not believe that any additional request detailing scope of work or timing commitments is necessary. If you disagree, as per our discussion with COL Lind, please provide an additional security expert to be available when our defense experts are not.

Best,  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
[coombs@armycourt martialdefense.com](mailto:coombs@armycourt martialdefense.com)  
[www.armycourt martialdefense.com](http://www.armycourt martialdefense.com)

## UNITED STATES

 $\gamma$ 

U.S. Army, xxx-xx-[REDACTED]

Army Garrison, Joint Base Myer-Henderson Hall,

Fort Myer, VA 22211

**REQUEST FOR  
RECONSIDERATION OF  
ADDENDUM #2 TO DEFENSE  
MOTION TO COMPEL  
DISCOVERY #2: REQUEST  
FOR WITNESSES**

21 June 2012

1. The Defense respectfully requests this Court reconsider its denial to produce certain witnesses for the Article 39(a) session on 25 June 2012 in light of the Government's 20 June 2012 submission.

2. The Defense requests that this Court order the Government to produce the following witnesses:

a) A witness from the Office of the National Counterintelligence Executive (ONCIX) who can testify to:

- i) the representation made to trial counsel in February 2012;
- ii) the representation made to trial counsel in March 2012;
- iii) what ONCIX had by way of a damage assessment in February and March 2012; and
- iv) the contents of the 18 May meeting with ODNI.

b) A witness from the Federal Bureau of Investigation (FBI) who can testify as to when the FBI had something by way of a damage assessment/impact statement, and when trial counsel had knowledge of this fact.

c) A witness from the Department of Homeland Security (DHS) who can testify as to when the DHS had something by way of a damage assessment, and when trial counsel had knowledge of this fact.



3. Given the timing of this reconsideration request, the Defense does not object to the Court considering telephonic testimony from a witness from each of the above agencies.<sup>1</sup>

#### FACTS

4. The Defense incorporates the factual assertions from its 18 June 2012 original request for witnesses. The Defense also requests the Court to consider the filing by the Government on 20 June 2012 (Prosecution Response to Defense Motion for Modified Relief for Defense Reply to Prosecution Response to Supplement to Defense Motion to Compel Discovery #2) and the statements by the Government during oral argument on 6 June 2012.

5. On 6 June 2012, the Defense argued its request for a due diligence accounting by the Government. After the Defense's argument, the Court asked the Government if it had a reply or whether it wanted to reserve its reply. MAJ Fein responded "...we would like to reserve our reply for the diligence argument since we did just receive it this past weekend." Article 39(a) Audio Recording 6 June 2012.

6. The Government allowed the Government a two-week extension to brief the issues raised in the Defense's motions for a due diligence accounting (e.g. the FBI impact statement; the ONCIX damage assessment, etc.).

7. During oral argument, the Court asked the Government to explain its representations concerning the FBI impact statement.

COURT: Alright, we will be addressing that aspect of this motion at the next session. I understand the Defense's argument. Government, are you prepared to tell me when you did know about this impact statement or impact assessment?

MAJ Fein: Your Honor, the Government would like to at least have a chance to argue the due diligence argument first and then answer that in (inaudible) Court's order.

Article 39(a) Audio Recording 6 June 2012.

8. MAJ Fein then proceeded to give the following lengthy statement:

MAJ Fein: But what the Government would say, at least is that, the Defense again is confusing, the Defense seems to confuse the issues of what authorities they have asked. Pre-Referral they asked for any impact or damage assessment and they listed the FBI in a general request under 701(a)(2). The Government replied "you're not entitled to that under that proper authority or proper legal basis or factual basis." So once the Government learned of it, then we started working the approvals. But the Government is prepared today, because I happen to know that answer, your Honor, is it was just a few weeks ago, in fact I think that it was three weeks ago, but again this is I think, I will, I can confirm it at a different time, that we received approval based off of our proposed

<sup>1</sup> "Over a party's objection, the military judge may authorize any witness to testify on interlocutory questions via remote means or similar technology if the practical difficulties of producing the witness outweigh the significance of the witness' personal appearance." R.C.M. 703(b)(1).

summaries, to turn it over to the Defense. In fact, the time it was, the time of the day we received it, I think was the 18<sup>th</sup> of May. Because that was the date we filed our 505(g)(2) for the other two damage assessments. So that was the day we received the approval, and then the next two days the Defense started objecting into this procedure we already litigated about disclosure of ex parte or not. At that point we needed to notify the FBI, like every other entity that might be entertaining giving approval under 505(g)(2) that this is the procedure that will likely occur. So that they can weigh that decision on how, how this Court is going to handle information in the future. And how they are going to disclose it or not. So since then your Honor, we have had the approval to turn it over. And as we have written in our motion there is no – the Defense even cited before, 701(a)(6) says as soon as practicable. As we cited, as we stated in our motions and on the record today, the moment this prosecution receives approvals to turn over information, unclass, classified, we as soon as possible, turn it over to the Defense. So, once we get it, we start working. This is an example of we didn't have a process in place. We notified the Defense and the Court in our filing, it's there. Once we have a process, and once we know how the Court wants to handle these, we are ready to go. And we can keep them ready to go.

*Id.*

9. Based upon MAJ Fein's lengthy response, the Defense again tried to focus the issue on when the Government knew about the FBI impact statement, and why it had not provided timely notice to the Court and the Defense:

Mr. Coombs: Okay, I guess if the Government is saying they found out about the FBI impact statement prior to or right at the time of their 18 May 2012 disclosures to this Court, then we have additional problems, based upon what the Government said about the FBI in that disclosure to this Court, indicating that they produce all classified and unclassified documents under 505(g)(1) that are relevant in this case with regards to the FBI. This goes back to the Government deciding on its own when it is going to enlighten the Court or the Defense when there is certain information out there. The Government became aware, now apparently from what he [MAJ Fein] just said, the Government was aware of or got approval to release this information on 18 May. So that still begs the question when they found out about it, but why are they not, at the very least, if they don't want to tell the Defense, they have to be alerting the Court to the existence of this information. What they are representing to the Court on 18 May is that they reviewed everything that is favorable to the accused or material to either guilt or punishment, and they have turned over everything. That is what they are representing on 18 May. If they were aware, obviously they were aware of this impact statement, they just didn't have authority apparently to turn it over. But, they should have stated in there, "oh by the way Ma'am, the FBI has an impact statement. We are currently working the process for approval to turn this over."

*Id.*

10. The Court once again asked the Government to provide clarification on when it knew about the FBI impact statement:

COURT: Alright, Government, what is your position on that?

MAJ Fein: Your Honor, we are trying to find the document.

Mr. Coombs: 18 May 2012. Prosecution disclosure to the Court.

[Court provides its copy to MAJ Fein]

COURT: Why don't you please announce for the record what appellate exhibit it is?

MAJ Fein: Yes your Honor, I have been handed Appellate Exhibit 125. I am also holding, what is this? So your Honor, I was just handed Appellate Exhibit 125 which is the prosecution disclosure to the Court on 18 May 2012, I am also holding because this will, it is a consistent application of your Honor of what the Government has been saying, the prosecution's response to the supplement to the Defense motion to compel discovery number 2 dated 31 May 2012. Which is Appellate Exhibit 100. Now, I am looking at page four of Appellate Exhibit 100, and page 2 of Appellate Exhibit 125.

COURT: Alright.

MAJ Fein: Your Honor, in both of these, the focus is, the Court's Order was to turn over forensic results and investigative files. This gets back to the issue that was already litigated last session. Investigative files have a specific terminology. We complied with the Court's Order and we disclosed it. As noted, to ensure the Court was properly informed and the Defense, in Appellate Exhibit 100 on page 4, the prosecution even gave notification, again about law enforcement files. And then in the second paragraph we also further requested that they search their entire records to disclose to the Court this information. It goes back to general requests and words do matter your Honor. The Government is not trying to play, to play fast and loose with terminology. We are trying to execute specifically what the Defense is requesting. It makes it much easier, we are told. And only once in pre-referral discovery, and as I have stated before, in a, in a, mass request was under 701(a)(2) any impact or damage from these organizations. We replied, "you did not provide an adequate basis, or legal basis, factual or legal basis," not "you are not entitled to it." It was never readdressed. We were on notice for Brady purposes. We started looking into it. We found it, we got approval, we notified on 18 May. Or, excuse me, on 31 May in this filing. And the prosecution is standing here today saying we are ready to actually turn over the summary to the Defense, once the Court reviews it, and if the Court authorizes the substitution. But it is not an investigative file. And although it is understandable that the FBI is the Federal Bureau of Investigation, it is a very large organization. It is a very large organization within the executive branch. The investigators are not directly tied to, and in fact, we were told by FBI headquarters that deals with the damage assessment, excuse me, the impact statement, that the investigating

office, the field office within the FBI, had no input or even contact with any aspect of the impact statement. It was a completely separate function.

*Id.*

11. Despite being given multiple opportunities to answer the question of when the Government was aware of the FBI impact statement, the Government never provided an answer to the Court.<sup>2</sup>

### ARGUMENT

12. During the 6-8 June motions hearing, the Government requested additional time to respond to the Defense's motion for a due diligence accounting. The Court granted the request. The purpose of the additional time was for the Government to respond to the questions of the Defense and the Court concerning what the Government knew and when concerning the ONCIX damage assessment, the FBI impact statement, and any other due diligence issues raised by the Defense's motions.

13. At oral argument, the Court asked MAJ Fein: "Government, are you prepared to tell me when you did know about this impact statement or impact assessment?" MAJ Fein's response was that he was *not* prepared to answer the question at the time, but would address this in the Government's written submission for which the Government requested (and was granted) a 2-week extension ("Your Honor, the Government would like to at least have a chance to argue the due diligence argument first and then answer that in (inaudible) Court's order."<sup>3</sup>).

14. The Government filed its submission yesterday, on 20 June 2012. The Government's submission fails to mention the FBI impact statement that MAJ Fein represented to the Court he would address in his submission. It also fails to mention the ONCIX damage assessment, the DHS damage assessment, the HQDA memo, the Department of State documents, etc. In short, the Government has not responded to a *single* issue raised by the Defense. Instead, the Government essentially asks the Court to, "trust us, we know what we are doing."

15. The whole point of allowing the Government two weeks to respond was to provide answers to the factual issues raised by the Defense, not to allow the Government to rehash arguments to the effect that there is no basis for ordering a due diligence statement. The Government already made *those exact same arguments* on 24 May 2012. See Appellate Exhibit XCVII (Prosecution Response to Defense Motion to Compel Discovery #2) ("The prosecution respectfully requests

---

<sup>2</sup> In its 22 March 2012 statement to the Court, the Government stated "the United States is concurrently working with other Federal Organizations which we have a good faith basis to believe may possess damage assessments or impact statements...." See Prosecution's Response to Court's Email Questions (22 March 2012). The Government undoubtedly knew of the FBI impact statement prior to its 22 March 2012 disclosure to the Court. The Government, however, failed to notify the Court on that date of the FBI impact statement. The Government also failed to notify the Court of the FBI impact statement on 20 April 2012 when it represented what the FBI had in its possession and that "the United States anticipates that the FBI is the only government entity that is a custodian of classified forensic results or investigative files relevant to this case that will seek limited disclosure IAW MRE 505(g)(2)." Appellate Exhibit LVI.

<sup>3</sup> The audio is inaudible at the end of MAJ Fein's statement; however, based on the context of the sentence, it is clear that MAJ Fein was deferring his answer until the Government's written submission.

that the Court deny the defense's request for the prosecution to respond to inquiries related to its due diligence search for discoverable information. There is no legal authority to support the defense's request. Should the Court be inclined to [grant the Defense's motion], the prosecution requests leave of the Court to require the prosecution to prepare internal memoranda and other attorney work-product, and present this information to the Court *ex parte* ... based on it being attorney work-product).

16. The purpose of deferring argument for two weeks was to enable the Government an opportunity to explain to the Court inconsistencies in the factual issues raised by Defense's motion. That is *the basis upon which* the Court granted a two-week extension. If the Government was going to use the two-week extension to simply regurgitate old arguments and repeat that "the prosecution continues to comply with its discovery obligations and will continue to do so" and "the prosecution has and continues to comply with its obligations under *Brady*" (See Government Response at p. 2), there was absolutely no need for this two-week extension.

17. It is clear that the Government has no plans to explain any of its conduct. It has not explained any of the following issues:

- a) Why didn't the Government tell the Court about the ONCIX damage assessment?
- b) Why did the Government represent that it had searched the files of 63 agencies prior to February 2012 and found no *Brady*, but now is saying that it did not begin its *Brady* search until February 2012 after ONCIX informed the Government that it needed to go to these agencies?
- c) When did the Government learn of the FBI impact statement? (not when did it get approval to tell the Defense). When did the FBI begin the impact statement? When did it complete the impact statement?
- d) When did the Government learn of the Department of Homeland Security damage assessment? Why didn't the Government tell the Court about this at the 6 June 2012 motions argument, given that the parties and the Court were in the process of discussing what damage assessments existed?
- e) Why didn't the Government ever follow-up with HQDA? Why did it take someone at HQDA, nine months after the original memo was circulated, to realize that nobody had conducted a *Brady* search?
- f) Why hadn't the Government already searched the files of the Department of State? How can it be that two years into the case, the only non-investigative document from the Department of State that the Government has seen is their Damage Assessment?
- g) Why has the Government not completed a *Brady* search of documents that it agrees are under military possession, custody and control?
- h) Why has the Government not yet completed a *Brady* search of closely aligned agencies?

At the upcoming oral argument, the Defense is certain that the Government will once again not provide any answers. Instead it will say (as it did at the last oral argument) something to the effect that it will "get back to the Court on that."

18. The Defense would also ask that the Court either read the limited transcriptions provided by the Defense in support of the request for witnesses or listen to the audio transcript itself. The

Government's responses are circular and evasive. It never once provides a direct answer – much less a believable answer – to any of the Court's questions.

19. In the Court's prior ruling that these witnesses were not "relevant and necessary" for the upcoming motions argument, the Defense assumes that the basis for this determination (at least in part) was that the Government would supply answers to the Court about the factual issues raised by the Defense. Thus, it was not necessary to ask questions of these witnesses because the Government would be supplying the answers in its submission. The Government has not done so, despite a two-week extension by the Court. The issues related ONCIX, the FBI, the HQDA memo, etc. *are not even mentioned* in the Government's submission.

20. The Defense believes that, in light of the Government's refusal to address even one of the factual issues raised by the Defense's motion and its evasive answers at the previous motions argument, these witnesses are now relevant and necessary to ascertain the factual predicate for the Government's diligence.

21. To anticipate a predictable argument by the Government, this Court should not defer its reconsideration of this issue until the next motions argument, as that would render the request moot. In other words, waiting until July to consider whether witnesses should appear for a June hearing (as the Government has suggested in the past) does not make sense. The Defense respectfully requests a timely ruling on this motion.

#### CONCLUSION

22. The Defense respectfully requests that this Court reconsider its ruling and order the Government to produce a witness from ONCIX, FBI, and DHS who can testify regarding the representations made to the trial counsel concerning any damage assessment/impact statement.

Respectfully submitted,



DAVID EDWARD COOMBS  
Civilian Defense Counsel

# ATTACHMENT

## David Coombs

---

**From:** David Coombs <coombs@armycourtartialdefense.com>  
**Sent:** Friday, June 15, 2012 5:44 PM  
**To:** 'Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA'; 'Overgaard, Angel M, CPT USA JFHQ-NCR/MDW SJA'; 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; 'Whyte, Jeffrey H, CPT USA JFHQ-NCR/MDW SJA'; Alexander.VonElten@jfhqncr.northcom.mil  
**Cc:** Hurley, Thomas F MAJ USARMY (US) (thomas.f.hurley4.mil@mail.mil); Tooman, Joshua J CPT USARMY (US)  
**Subject:** Update

Ashden,

Please provide feedback on the following:

- 1) Article 39(a): Please have PFC Manning at the courthouse at 0900 on 25 June. I want to be able to go over some documentation with him.
- 2) Case Calendar: Are you planning on submitting a case calendar or commenting on the calendar the Defense submitted on Monday? If so, when?
- 3) Motions: When is the Government filing its Due Diligence response motion and its targeted brief on damage?
- 4) Sanitized Versions: Do you have an update on being able to provide unclassified versions of the various damage assessments?
- 5) Department of Homeland Security Damage Assessment: Have you sent this to the NWC?
- 6) Redactions: Are you still planning on submitting your response tomorrow – or did you mean today?
- 7) Replacement for Santiago: TDS does not have the ability to provide a replacement warrant officer for CW2 Santiago. Can the Government provide a suitable replacement?

Best,  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
[coombs@armycourtartialdefense.com](mailto:coombs@armycourtartialdefense.com)  
[www.armycourtartialdefense.com](http://www.armycourtartialdefense.com)



**David Coombs**

---

**From:** Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA <Ashden.Fein@jfhqncr.northcom.mil>  
**Sent:** Friday, June 15, 2012 6:12 PM  
**To:** David Coombs  
**Cc:** Hurley, Thomas F MAJ USARMY (US); Tooman, Joshua J CPT USARMY (US); Santiago, Melissa S CW2 USARMY (US); Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA; Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA; Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA; von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA; Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA  
**Subject:** Update

David,

Below is an update on your questions and other issues.

1. Article 39(a). We will have PFC Manning at the courthouse at 0900 on 25 June.
2. Case Calendar. We intend to submit a case calendar update on Thursday with our other filings.
3. Motions. We intend to submit our two filings on Thursday, as per our discussion last week.
4. Sanitized Versions of Damage Assessments. We have provided the defense all the damage/impact assessments that exist within each agency or organization. The government did not produce unclassified versions of the damage assessments for the ones that are classified and which have been produced; therefore, there are no unclassified or sanitized versions to provide.
5. Department of Homeland Security Damage Assessment. As stated on Friday, we sent the request earlier this week and NWC received it on Wednesday. Additionally, CW2 Santiago signed for a copy on Wednesday. I apologize for not notifying you sooner of the tracking number or confirmed delivery.
6. Redactions. We will file with the Court tonight and we do not intend to request protective orders.
7. Replacement for Santiago. As previously stated, MDW was informed that the Chief, TDS coordinated directly or indirectly with you for personnel issues concerning the defense. After confirming with the Chief Warrant Officer of the Corps, it is our understanding that all future personnel requests for any personnel, will be handled through TDS channels. Please address any personnel issues through the military defense counsel and their RDC.
8. Defense Expert Request. We have not resolved the issue of the defense requesting that your experts have their time dedicated primarily to the defense. Does the defense intend to request this? Without a request which outlines the anticipated scope of their additional duties (which is already written in your proposed memo) and an estimate of the total time you anticipate you will need their services, we cannot go to their leadership and the convening authority for approval. The leaders must know how much time you anticipate will be needed and to what extent, so they can make informed decisions. Once we receive a request, we will immediately take the request to your experts' leadership and the convening authority for action.

Have a good weekend.

**David Coombs**

---

**From:** David Coombs <coombs@armycourtartialdefense.com>  
**Sent:** Friday, June 15, 2012 6:31 PM  
**To:** 'Fein, Ashden MAJ USA JFHQ-NCR/MDW SJA'; 'Hurley, Thomas F MAJ USARMY (US)'; 'Tooman, Joshua J CPT USARMY (US)'; 'Santiago, Melissa S CW2 USARMY (US)'; 'Morrow III, JoDean, CPT USA JFHQ-NCR/MDW SJA'; 'Overgaard, Angel M. CPT USA JFHQ-NCR/MDW SJA'; 'Whyte, Jeffrey H. CPT USA JFHQ-NCR/MDW SJA'; 'von Elten, Alexander S. CPT USA JFHQ-NCR/MDW SJA'; 'Ford, Arthur D. CW2 USA JFHQ-NCR/MDW SJA'  
**Subject:** RE: Update

Ashden,

- 1) Thank you.
- 2) Why do you feel that Thursday is the agreed upon date for the case calendar?
- 3) Same as #2 - I don't recall any discussion that Thursday was the timeline for this issue. Not only would this give no time for the Defense to reply, it also does not provide the Court with time to consider the motions prior to the Article 39(a).
- 4) The Defense is requesting that the various agencies produce an unclassified version of their damage assessments. According to the defense security experts, this is not an unusual request.
- 5) Not a problem. Thank you.
- 6) Thank you.
- 7) As stated, TDS cannot provide a replacement warrant officer. I am requesting that the Government provide a replacement for CW2 Santiago. Please inform me if the Government's position is that it will not do so.
- 8) The Defense does not believe that any additional request detailing scope of work or timing commitments is necessary. If you disagree, as per our discussion with COL Lind, please provide an additional security expert to be available when our defense experts are not.

Best,  
David

David E. Coombs, Esq.  
Law Office of David E. Coombs  
11 South Angell Street, #317  
Providence, RI 02906  
Toll Free: 1-800-588-4156  
Local: (508) 689-4616  
Fax: (508) 689-9282  
[coombs@armycourtartialdefense.com](mailto:coombs@armycourtartialdefense.com)  
[www.armycourtartialdefense.com](http://www.armycourtartialdefense.com)

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

Prosecution Response  
to Defense Motion to Request  
Reconsideration of Addendum #2 to  
Defense Motion to Compel Discovery #2:  
Request for Witnesses

21 June 2012

### RELIEF SOUGHT

The prosecution respectfully requests that the Court deny the defense's motion for reconsideration.

### BURDEN OF PERSUASION AND BURDEN OF PROOF

The burden of proof on any factual issue the resolution of which is necessary to decide a motion shall be by preponderance of the evidence. RCM 905(c)(1). The burden of persuasion on any factual issue the resolution of which is necessary to decide a motion shall be on the moving party. RCM 905(c)(2).

### FACTS

On Saturday, 2 June 2012, the defense filed a "defense motion for modified relief" requesting the Court suspend the proceedings pending a due diligence statement. See Appellate Exhibit C1.

During the 6 June 2012 Article 39(a) session the Court asked the government whether the government requested to reserve replying to the defense's due diligence argument until the next motions hearing. See Session Audio, 12:09:18 - 12:09:38 ("would you like to reserve replying or do you have any reply you would like to address the Court at this time - or both?"). The government responded that based on receiving the motion the weekend before, the government would like to reserve a response to the due diligence argument. See *Id.* ("...your Honor, looking at the time, we would like to reserve a reply to the diligence argument because we just received it this weekend...").

On 18 June 2012, the defense submitted a request for witnesses via email to the Court requesting witnesses from the Office of the National Counterintelligence Executive (ONCIX), the Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS) for the Article 39(a) session on 25 June 2012. See Defense Motion, dated 18 June 2012.

On 19 June 2012, the Court denied the defense motion to produce witnesses finding the witnesses not relevant and necessary for the Court to rule on the defense's due diligence motion. The Court also found the motion to be untimely. See Court Order, dated 19 June 2012.

### WITNESSES/EVIDENCE

The prosecution does not request any witnesses or evidence be produced for this motion. The prosecution requests that the Court consider the Appellate Exhibit, audio session, and filings referenced herein.

### LEGAL AUTHORITY AND ARGUMENT

The United States objects to the Court's reconsideration of its ruling that the witnesses are not relevant and necessary and that the defense's request was untimely. On 2 June 2012, the defense motioned the Court to require the government to provide a diligence statement and, at the motions hearing on 6 June 2012, the government requested time to respond to whether the government should be required to provide a due diligence statement to the Court. Furthermore, after being asked by the Court to provide specific dates on when the government received certain information, the government requested to defer answering the Court's questions about timing, until the due diligence statement motion was completely litigated.

On 20 June 2012, the government filed its response to the due diligence motion arguing that the Court should not order the government to provide a response, thus potentially making this issue moot, or in the alternative the government file a response *ex parte*. The government recognizes, that if after consideration of both parties argument (for which the defense has already argued), the Court orders the government to produce a statement, then the government will comply with the Court's order.

### CONCLUSION

The prosecution respectfully requests that the Court deny the defense's motion for reconsideration.



ASHDEN FEIN  
MAJ, JA  
Trial Counsel

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 21 June 2012.



ASHDEN FEIN  
MAJ, JA  
Trial Counsel

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC  
U.S. Army, xxx-xx-  
Headquarters and Headquarters Company,  
U.S. Army Garrison, Joint Base Myer-  
Henderson Hall, Fort Myer, VA 22211

)  
)  
) ORDER: DEFENSE  
) MOTION TO  
) RECONSIDER WITNESS  
) PRODUCTION

) DATED: 21 June 2012  
)

The Court considered the Defense Motion to Reconsider production of witnesses from the Federal Bureau of Investigation (FBI), Office of the National Counterintelligence Executive (ONCIX), and Department of Homeland Security (DHA) for the Article 39(a) session on 25 June 2012. The Defense motion is untimely. These witnesses are not relevant and necessary for the Court to rule on the Due Diligence Motion. The Defense Motion to produce witnesses is Denied.

So ORDERED: this 21<sup>st</sup> day of June 2012.



DENISE R. LIND  
COL, JA  
Chief Judge, 1<sup>st</sup> Judicial Circuit

Appellate Exhibit 156

3 pages

classified

"SECRET"

ordered sealed for Reason 2  
and Reason 7 (government)

Military Judge's Seal Order  
dated 20 August 2013

stored in the classified  
supplement to the original  
Record of Trial

Appellate Exhibit 156

Enclosure 1

27 pages

classified

"SECRET"

ordered sealed for Reason 2  
and Reason 7 (government)

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial

Appellate Exhibit 156

Enclosure 2

27 pages

classified

"SECRET"

ordered sealed for Reason 2  
and Reason 7 (government)

Military Judge's Seal Order

dated 20 August 2013

stored in the classified

supplement to the original

Record of Trial



Appellate Exhibit 156

Enclosure 3

2 pages

classified

"SECRET"

ordered sealed for Reason 2  
and Reason 7 (government)

Military Judge's Seal Order  
dated 20 August 2013

stored in the classified  
supplement to the original  
Record of Trial

IN THE UNITED STATES ARMY  
FIRST JUDICIAL CIRCUIT

UNITED STATES

v.

MANNING, Bradley E., PFC  
HHC, U.S. Army Garrison  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

CLASSIFIED INFORMATION  
SEAL ORDER

DATED: \_\_\_\_\_

1. The following exhibit \_\_\_\_\_ contains classified information as defined in MRE 505(b). The exhibit is classified at the SECRET//NOFORN level. This exhibit will be sealed in the record of trial in accordance with RCM 1103A, RCM 1104(b)(1)(D), and MRE 505. The classified enclosures will be sealed separately in the location stated in the exhibit in accordance with RCM 1103A, RCM 1104(b)(1)(D), and MRE 505.

2. The Court Security Officer shall cause a proper security classification to be assigned to the record of trial, to each classified exhibit, and to each page of the record of trial in which classified information appears, in accordance with RCM 1103(h). The Court Security Officer will ensure that the sealed exhibits are properly marked, including an annotation on each, that the material was sealed by order of the military judge prior to insertion into the original record of trial. Trial counsel will clearly identify in the record of trial where classified exhibits and pages in the record of trial will be maintained.

3. This exhibit and pages contain classified national security information. This classified information shall be handled in a manner consistent with Executive Order 13526. An individual's access to the classified information in this exhibits and pages is subject to the following: having the appropriate security clearance; signing an approved nondisclosure agreement; having a need-to-know the information; and acknowledging the Judicial Protective Order for Classified Information, dated 16 March 2012.

4. Sealed exhibits will not be opened or examined except for the following:

a. Prior to authentication of the record by the military judge, sealed materials may be examined upon order from the military judge based on good cause.

b. After authentication and prior to disposition of the record of trial pursuant to RCM 1111, sealed materials may be examined upon order issued from the military judge upon a showing of good cause at a post-trial Article 39(a) session directed by the Convening Authority.

c. Reviewing and appellate authorities meeting the criteria in paragraph 3 may examine sealed matters when those authorities determine that such action is reasonably necessary to a proper fulfillment of their responsibilities under the Uniform Code of Military Justice, the Manual for Courts-Martial, governing directives, instructions, regulations, and applicable rules of professional responsibility.

5. No person authorized to examine sealed exhibits shall photocopy, photograph, duplicate, or disclose the contents of the sealed exhibit in the absence from an order by a military judge, the Judge Advocate General or designee, or an appellate court, or other court of competent jurisdiction.

ORDERED, this the \_\_\_\_\_ day of \_\_\_\_\_ 2012.

DENISE R. LIND  
COL, JA  
Chief Judge, 1st Judicial Circuit

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

Prosecution Disclosure  
to the Defense

22 June 2012

On 22 June 2012, the United States filed an *ex parte* motion requesting the Court consider that motion *in camera* and *ex parte* under MRE 505(g)(2) and to authorize a substitution of the portion of the Federal Bureau of Investigation (FBI) impact statement that is favorable to the accused and material to guilt or punishment under MRE 505(g)(2)(A) and (B). See Enclosure. The United States seeks to protect information relating to intelligence activities (including covert action), intelligence sources or methods, or cryptology, all within the national security interests of the United States.



ASHDEN FEIN  
MAJ, JA  
Trial Counsel

Enclosure

Government *ex parte* Motion (unclassified redacted version)

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Government *in camera* Motion for  
Authorization of a Substitution of  
the FBI Impact Statement  
under MRE 505(g)(2)

22 June 2012

RELIEF SOUGHT

(U) COMES NOW the United States of America, by and through undersigned counsel, respectfully requests this Court to: (1) consider this motion *in camera* and *ex parte* under MRE 505(g)(2); and (2) authorize a substitution of the portion of the Federal Bureau of Investigation (FBI) impact statement that is favorable to the accused and material to guilt or punishment under MRE 505(g)(2).

BURDEN OF PERSUASION AND BURDEN OF PROOF

(U) As the moving party, the United States has the burden of persuasion on any factual issue the resolution of which is necessary to decide the motion. Rule for Courts-Martial (RCM) 905(c)(2). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

FACTS

[REDACTED]

(U) The FBI is an agency outside the Department of Defense. The FBI approved the release of the impact statement; however, they requested some portions be redacted and summarized. See Enclosure 3.

(U) The FBI authorizes the prosecution to produce the summarized impact statement to the defense counsel in classified discovery. The defense counsel and their experts are not authorized to share the information contained within the report or their notes with the accused. See Enclosure 3.

WITNESSES/EVIDENCE

(U) The United States does not request any witnesses be produced for this motion. The prosecution requests that the Court consider the enclosures listed at the end of this motion.

## LEGAL AUTHORITY AND ARGUMENT

(U) If classified information is at issue in a court-martial, then the United States may agree to disclose the classified information to the defense under a protective order. See MRE 505(g)(1). Additionally, the United States may motion the Court to "authorize (A) the deletion of specific items of classified information from documents to be made available to the [accused], (B) the substitution of a portion or summary of the information for classified documents, or (C) the substitution of a statement admitting relevant facts that the classified information would tend to prove." MRE 505(g)(2). The military judge "shall authorize" these alternative forms, unless she determines "the disclosure of the classified information itself is necessary to enable the accused to prepare for trial." *Id.* If a motion is filed under MRE 505(g)(2), then upon request of the United States, the motion "shall" be considered by the military judge *in camera* and "shall not be disclosed to the accused." *Id.*

(U) The procedures outlined in MRE 505(g)(1) and (2) apply when the United States voluntarily discloses information and does not withhold classified information under MRE 505(c). If the United States intends to withhold information under MRE 505(c), then the United States must move for an *in camera* proceeding under MRE 505(i)(2), obtain an affidavit demonstrating that disclosure of the information reasonably could be expected to cause damage to the national security under MRE 505(i)(3), and follow the notice procedures outlined under MRE 505(i)(4). See MRE 505(i). For the purposes of this filing, the FBI, through the prosecution, is voluntarily disclosing the impact statement with redactions and summarizations and is not withholding any classified information under MRE 505(c) and MRE 505(i).

██████████ The prosecution reviewed the original ██████████ impact statement for information favorable to the accused and material to guilt or punishment. See RCM 701(a)(6); see also *Brady v. Maryland*, 373 U.S. 83 (1963). The prosecution reviewed the original FBI impact statement and determined that it contained information that was favorable to the accused and material to guilt or punishment. The particular sections are highlighted in yellow. See Enclosure 1. The prosecution identified discoverable information and the FBI reviewed the information to determine if it would authorize the prosecution to voluntarily disclose the original classified material to the defense under MRE 505(g)(1) or (g)(2). The FBI determined it would disclose the information in summarized form with redactions under MRE 505(g)(2). ██████████

██████████ The prosecution reviewed the redactions and summarizations and determined that they accurately summarized the original discoverable material, including providing adequate context.

(U) The information contained within the original report, which is redacted, does not meet the RCM 701(a)(6) or *Brady/Giglio* standards and therefore is not discoverable, nor is it material to the preparation of the defense or relevant and necessary for production under RCM 703(f). Additionally, that information is not "necessary to enable the accused to prepare for trial" under MRE 505(g)(2). Therefore, the defense is not entitled to discovery of the redacted information.

(U) Should the Court find the deleted, substituted, or summarized information is discoverable under RCM 701(a)(6), or *Brady/Giglio*, relevant and necessary for production under RCM 703(f), or is "necessary to enable the accused to prepare for trial" under MRE 505(g)(2), then the United States requests the opportunity to either: (1) address the Court's findings with the relevant government agency to determine whether a different alternative under MRE 505(g)(2) is appropriate and file that alternative with the Court, or (2) allow for the relevant government agency to claim a privilege under MRE 505(c) and the United States to move for an *in camera* proceeding under MRE 505(i).

[REDACTED]

(U) The prosecution will not use any portion of the FBI impact statement not disclosed to the defense during any portion of the trial. This includes rebuttal and rule of completeness if the defense introduces or references anything in the substitution. If the prosecution does offer aggravating evidence during the presentencing portion of the trial, then it will disclose the evidence pursuant to RCM 701(a)(5), subject to any required protections under MRE 505.

CONCLUSION

(U) The United States respectfully requests this Court to: (1) consider this motion *in camera* and *ex parte* under MRE 505(g)(2), and (2) authorize a substitution of the portion of the FBI impact statement that is favorable to the accused and material to guilt or punishment under MRE 505(g)(2).



ASHDEN FEIN  
MAJ, JA  
Trial Counsel

4 Enclosures

1. Original FBI Impact Statement (classified [REDACTED])
2. Redacted and Summarized FBI Impact Statement (classified [REDACTED])
3. FBI Memorandum, dated 19 June 2012 (classified [REDACTED])
4. Draft Sealing Order

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Prosecution Supplement to  
Prosecution Motion  
for Appropriate Relief  
to Preclude Actual Harm or Damage  
from the Pretrial Motions Practice  
and the Merits Portion of the Trial

21 June 2012

RELIEF SOUGHT

The Government respectfully requests that the Court preclude the defense from raising or eliciting any discussion, reference, or argument, to include the introduction of any documentary or testimonial evidence, relating to actual harm or damage, or lack thereof, from pretrial motions related to the merits portion of trial and from the merits portion of trial. The Government does not dispute whether actual harm or damage, or lack thereof, is relevant on sentencing.

This filing is in response to the Court's request for a brief discussing whether later events are relevant to a prior determination of what could occur. The Court requested that the brief include relevant case law. In particular, the Court requested the parties submit case law discussing assault with respect to injuries and causation. The Government submits that both the assault hypothetical raised by the Defense at oral argument and case law conclusively demonstrate that after-the-fact evidence of damage is irrelevant and should therefore be precluded.

BURDEN OF PERSUASION AND BURDEN OF PROOF

As the moving party, the prosecution bears the burden of persuasion and must prove any factual issues necessary to decide this motion by a preponderance of the evidence. See Manual for Courts-Martial (MCM), United States, Rule for Court-Martial (RCM) 905(c) (2012).

FACTS

The Government relies on the facts it stated in its Motion for Appropriate Relief to Preclude Actual Harm or Damage from the Pretrial Motions Practice and the Merits Portion of the Trial (Prosecution Motion).

WITNESSES/EVIDENCE

The Government does not request any witnesses be produced for this response. The Government respectfully requests that the Court consider the Prosecution Motion.

APPELLATE EXHIBIT 158  
PAGE REFERENCED: \_\_\_\_\_  
PAGE \_\_\_\_ OF \_\_\_\_ PAGES

## LEGAL AUTHORITY AND ARGUMENT

After-the-fact evidence is irrelevant to prior events. A determination of “what could happen” is not affected by what actually happens in the future. Any damage or harm that occurred happened after commission of the charged acts, thereby making all damage irrelevant. Evidence is relevant if it has “any tendency to make the existence of any fact that is of consequence to the determination of the action more probable . . . than it would be without the evidence.” *United States v. Tanner*, 63 M.J. 445, 449 (C.A.A.F. 2006) quoting Military Rule of Evidence (MRE) 401. The military judge may exclude irrelevant evidence. *See United States v. Israel*, 60 M.J. 485, 489 (C.A.A.F. 2005). After-the-fact evidence is irrelevant to a person’s intent and state of mind at an earlier time. *See Gulbranson v. Duluth, Missabe & Iron Range Ry. Co.*, 921 F.2d 139, 142 (9th Cir. 1990). Actual harm or damage, including any lack thereof, is irrelevant because the Government need not prove actual damage. Additionally, actual harm or damage, or lack thereof, is irrelevant to the accused’s intent because it occurred after commission of the charged acts. Finally, actual harm or damage is irrelevant to any proof of whether the compromised information was entitled to protection or could injure the United States, including those specifications charging violations of §§ 793(e) and 1030(a)(1), and Articles 104 and 134, because any harm or its absence occurred after the charged acts. Accordingly, the Government requests that the Prosecution Motion be granted.

### I. AFTER-THE-FACT DAMAGE IS IRRELEVANT ON THE MERITS

After-the-fact evidence does not establish potential danger. *See Whitley v. Albers*, 475 U.S. 312, 323 (determining that infliction of pain does not amount to cruel and unusual punishment because it may appear in retrospect that the degree of force authorized was unnecessary when determining whether use of force during prison riot was wanton and unnecessary). “An expert’s after-the-fact opinion that danger was not ‘imminent’ in no way establishes that there was no danger, or that a conclusion by the officers that it was imminent would have been wholly unreasonable.” *Id.* (emphasis in original). Furthermore, an after-the-fact assessment is irrelevant because the facts are examined as they appeared to the accused at the time of the charged criminal act. *See Fennel v. Gilstrap*, 559 F.3d 1212, 1218 (11th Cir. 2009) (declining to consider the conclusions of an investigation conducted after the use of force against a pretrial detainee).

Additional case law supports the Government’s argument that after-the-fact evidence is irrelevant to a person’s intent and state of mind at an earlier time. *See Gulbranson* at 921 F.2d at 142 (deciding that railroad’s awareness of problem in 1985 not relevant to its knowledge of the problem in 1984) citing *Tallarico v. Trans World Airlines, Inc.*, 881 F.2d 566, 572 (8th Cir. 1989). In particular, after-the-fact evidence is not probative to state of mind for personal injury cases. *See, e.g., Arnold v. Riddell, Inc.*, 882 F. Supp. 979, 993 (D. Kan. 1995) (determining video made six years after injury is irrelevant to prove warnings available in product liability case); *Sealover v. Carey Canada*, 793 F. Supp. 569, 579 (M.D. Pa. 1992) (excluding evidence that manufacturer had knowledge of health risks posed by its product in 1961-62 where plaintiff had to prove manufacturer had knowledge prior to 1960). Similarly, after-the-fact opinions are disfavored in discrimination cases; courts permit “pretext” to attack after-the-fact justifications



for employee termination. See, e.g., *See Santiago-Ramos V. Centennial P.R. Wireless Corp.*, 217 F.3d 46 (1st Cir. 2000) citing *Mariani Giron v. Acevedo Ruiz*, 834 F.2d 238, 239 (1st Cir.1987).

II. DAMAGE IS IRRELEVANT BECAUSE IT OCCURRED AFTER THE ACCUSED FORMED HIS INTENT

A. Actual Harm or Damage Is Irrelevant to the Accused's Intent

Unlike any other in the criminal code, the Espionage Act sanctions prior restraint to prevent substantive evils that, in Justice Oliver Wendell Holmes's words, "create a clear and present danger." See *United States v. Schenck*, 249 U.S. 47, 52 (1919); see also Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information*, 73 Colum. L. Rev. 929, 941 (1973) (describing the criminalization of information gathering). The Espionage Act protects the secrecy necessary to conduct certain governmental functions, including defense and diplomacy. See *New York Times Co. v. United States*, 403 U.S. 713, 728 (1971) (Stewart, J., concurring) ("[I]t is elementary that the successful conduct of international diplomacy and the maintenance of an effective national defense require both confidentiality and secrecy."). Under the Espionage Act, criminal defendants have been convicted in undercover operations and for conspiracy charges where no actual harm to the national security ever occurred. See, e.g., *United States v. Miller*, 874 F.2d 1255 (9th Cir. 1989). To the Government's knowledge, no court has ever permitted evidence pertaining to actual damage or injury during a trial, nor charged a jury with requiring the Government to establish actual harm or damage. Accordingly, the Government does not need to prove actual harm or damage to satisfy the requirements of § 793(e) nor § 1030(a)(1). See *Gorin v. United States*, 312 U.S. 19, 29 (1941); Charge Sheet.

Instead, the Government need only prove that the documents *could* be used to the injury of the United States, not that the charged documents<sup>1</sup> *would* be used to the injury of the United States or did injure the United States.<sup>2</sup> See *United States v. Allen*, 31 M.J. 572, 628 (N.M.C.M.R. 1990). To prove the requisite *mens rea*, the Government must demonstrate that the accused was aware or should have been aware of the potential for the information to be used to the injury of the United States.<sup>3</sup> See *United States v. Diaz*, 69 M.J. 127, 133-34; 133 n. 4 (C.A.A.F. 2010). Additionally, an altruistic or innocent purpose does not negate culpability. See *Allen*, 31 M.J. at 628 ("[T]he espionage act implies that information shall not be given even to an ally regardless

<sup>1</sup> §§ 793(e) and 1030(a)(1) apply to documents broadly defined and information. Throughout this Supplement, the Government refers to information and documents interchangeably, including the charged documents. The distinction is moot given the CAAF's ruling in *Diaz*, which held that information improperly disseminated under § 793(e) was not subject to a heightened bad faith *scienter*, thereby eliminating the distinction between "documents" and "information" created in *United States v. Rosen*, 445 F. Supp.2d 602, 626 (E.D. Va 2006). See generally *United States v. Steele*, 2011 WL 414992 at \*4 (A. Ct. Crim. App. 3 February 2011) citing *United States v. Diaz*, 69 M.J. 127, 132-33 (C.A.A.F. 2010).

<sup>2</sup> For the sake of brevity, this Supplement will refer "to the injury of the United States" in place of "to the injury of the United States or advantage of any foreign nation."

<sup>3</sup> The phrase "which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation" only modifies "information relating to the national defense." See Enclosure at 7 (discussing the scope of § 793(d) in the legislative history).

of how innocent, or commendable a purpose the person disclosing the information had.”) citing *United States v. Heine*, 151 F.2d 813, 815 (2d Cir. 1945). Furthermore, any current lack of damage is neither indicative nor predictive of harm that could arise in the future. To be relevant, the Defense’s theory requires adding “relations back” to national security law.

Contrary to the Government’s arguments in the Prosecution Motion, the Defense claims that an alleged absence of harm is relevant to three offenses: § 793(e), § 1030(a)(1), and Article 134, UCMJ. See Defense Response to Prosecution Motion to Preclude Reference to Actual Harm or Damage (Defense Response) § 11(a). Stating its relevance argument, the Defense bases its contention on the intent element of the three offenses, namely, under §§ 793(e) and 1030(a)(1) that the accused had reason to believe the compromised information could be used to the injury of the United States, and, under Article 134, that the accused acted “wantonly.” See Defense Response ¶¶ 13-14. However, the Defense argument fails because it seeks to prove intent with facts occurring after the accused formed his intent. Because Congress amended § 1030(a)(1) in 1996 to track more closely the language of § 793(e), the following analysis discussing § 793(e) applies equally to § 1030(a)(1). See S. Rep. No. 104-357 at 6 (1996).

The relevant intent is the accused’s state of mind at the precise moment he committed the charged acts. See *Holloway v. United States*, 526 U.S. 1, 8; U.S. Dept. of Army. Pam. 27-9, Military Judges’ Benchbook, (1 January 2010) (5-11-1) (Benchbook); see also Benchbook (5-11-2). In *Holloway*, the Supreme Court decided whether a carjacking statute required a specific and unconditional intent. See *id.* at 6-7. In relevant part, the statute read, “Whoever, with intent to cause death or serious bodily harm takes a motor vehicle . . . from the person or presence of another by force and violence or by intimidation, or attempts to do so, shall . . .” *Id.* at 3 n. 1 citing 18 U.S.C. § 2119 (1994 & Supp. III) (emphasis in original omitted). The Supreme Court determined that the *mens rea* of “the intent to cause death or seriously bodily harm” modified the act of taking. *Id.* at 8 (considering the placement of the *mens rea* with respect to the *actus reus*). In particular, the Court found that the statute directed the factfinder’s attention to the accused’s state of mind at the precise moment he demanded control of the car. *Id.* Thus, the intent is measured at the time the criminal act is committed.

Here, under §§ 793(e) and 1030(a)(1), the intent is measured at the precise moment when the compromised documents were communicated, delivered, transmitted, or caused to be the same. See *id.* at 6-7; see also *Brown v. Gardner*, 513 U.S. 114, 118 (1994) (“[T]he meaning of statutory language, plain or not, depends on context.”). In pertinent part, § 793(e) states, “which information the possessor has reason to believe.” The intent is possessed at the moment the accused willfully transmits, communicates, or delivers the compromised documents under a plain reading of the statute. Similarly, § 1030(a)(1), in relevant part, states that “with reason to believe.” Again, the intent is possessed at the time of transmission, communication, or delivery of the compromised documents. This analysis applies equally to the “wantonly” intent charged under Article 134. The degree of carelessness of wanton acts is determined at the time of the act; subsequent events do not alter it. See *Holloway, supra*; Benchbook (5-11-1, 5-11-2). The accused’s reason to believe whether the documents could be used to the injury to the United States, therefore, is considered at the moment of communication, transmission, or delivery of the documents. Later harm, or lack thereof, has no bearing on the *mens rea* or its termination, and any later harm does not make the *mens rea* more or less probable. See MRE 401.

Because the facts alleged by the defense were unknown to the accused at the moment he formed his intent, they could not have affected his intent and are therefore irrelevant. A § 793 violation under the Espionage Act does not require establishing that the accused acted with the bad faith of believing that the United States *would* be harmed. See *Miller*, 874 F.2d at 1278 n. 15. The after-the fact damage is also irrelevant to a mistake of fact defense for both specific and general intent crimes. As with intent in *Holloway*, the focus is on the precise moment the accused commits the charged acts. See Benchbook (5-11-1) (“If the accused *at the time of the offense* was (ignorant of the fact) (under the mistaken belief) then he cannot be found guilty of the offense(s) . . . .”) (emphasis added); Benchbook (5-11-2) (“[I]f you are convinced beyond a reasonable that, *at the time of the charged offense(s)*, the accused’s (ignorance) (mistake) was unreasonable, the defense of (ignorance) (mistake) does not exist.”) (emphasis added). Consequently, the irrelevant evidence must be precluded.

#### B. Actual Harm Is Irrelevant to Proof that the Information Could Cause Injury to the United States

Factors, including classification of the documents and expert testimony of the potential damage from disclosure of the documents to unauthorized persons, determine whether the information could be used to the injury of the United States. See *Gorin*, 312 U.S. at 29; *Diaz*, 69 M.J. at 133. Proof of classification constitutes evidence that the compromised information could be used to the injury of the United States.<sup>4</sup> See *Diaz*, 69 M.J. at 133 (“Surely classification may demonstrate that an accused has reason to believe that the information relates to national defense and could cause harm to the United States.”). Documents are classified if their unauthorized disclosure reasonably could be expected to result in damage to the national security. See Exec. Order No. 13526 § 1.1(4); *Gorin*, 312 U.S. at 28 (determining that the term “national defense” as used in a predecessor to § 793 is a broad concept); *United States v. Morison*, 844 F.2d 1057, 1071, 74 (4th Cir. 1988) (noting that national defense information is information that is potentially damaging to the United States). Additionally, § 1030(a)(1) protects information that has been explicitly determined by the United States to be information that could be used to the injury of the United States. § 18 U.S.C. § 1030(a)(1) (2012).

Determinations of whether the document could be expected to cause damage to the national security are based on the information and circumstances known at the time of the classification decision. See *United States v. Abu-Jihaad*, 630 F.3d 102, 112 (2d Cir. 2010) citing *United States v. Abu-Jihaad*, 600 F. Supp.2d 362, 377 (D. Conn. 2009) (noting that Navy operational instructions should be classified until after deployment or a visit had been approved by the host government). However, a document need not be classified to be protected under espionage laws; national defense information also receives protection under the Espionage Act. See *United States v. Squillacote*, 221 F.3d 542, 575-76 (4th Cir. 2000). National defense information (NDI) is a term of “broad connotations, referring to the military and naval establishments and the related activities of national preparedness.” See *Gorin*, 312, U.S. at 28. Under the Espionage Act, unclassified NDI is protected from disclosure if it is closely held by the Government. See *Squillacote*, 221 F.3d at 575-76, 578 (noting that a document containing

---

<sup>4</sup> Under military law, classification is not sufficient by itself nor is it the only means by which information can be shown to be the kind that could be used to the injury of the United States. See *Diaz*, 69 M.J. at 133.

NDI “will not be considered available to the public (and therefore no longer [NDI]) until the official information in that document is lawfully available.”) (emphasis in original). Accordingly, information that could be used to the injury of the United States includes unclassified NDI. *See Gorin; Squillacote, supra.*

The Defense relies on two additional, albeit related, arguments to justify inclusion of actual harm on the merits by attacking classification. First, the Defense contends that it “is entitled to argue that, by virtue of his expertise and training, [the accused] knew which documents and information could be used to the injury of the United States or to the advantage of any foreign nation.” Defense Response ¶ 15. The Defense is entitled to invoke a mistake of fact defense; however, the defense is limited to the circumstances at the time of the mistake. Second, the Defense states that the alleged “absence of damage is relevant for the impeachment of Government witnesses who claim that the leaks ‘could’ cause damage.” *Id.* at ¶ 19. The Espionage Act criminalizes the *act* of transmitting or retaining national defense information without consideration of any damage that might ensue. *See Gorin; Squillacote, supra.* Under the Defense’s theory, the accused could escape criminal responsibility for disclosure of national defense information because the Government was not able to quantify with precision any damage that may accrue *in the future* despite no statutory requirement to prove any harm or damage.<sup>5</sup>

The Defense’s first argument fails because the accused does not make the determination whether compromise of the information could injure the United States with respect to classification. *Cf. United States v. Zettl*, 889 F.2d 51, 53 (4th Cir. 1989) (“Even those with authority to see and handle the documents have no right without authority to convey the documents to others, whether or not the other party may have a need to know the information therein. Any other holding would make the possessor of any classified document the ultimate authority in deciding whether or not the document should be transferred to someone else. This, however, is a function of the government and its system of accountability for classified documents, not of someone who just happens to be in possession thereof, whether or not he rightfully possesses the document.”). Classification authority, including the authority to declassify information, belongs to an original classification authority (OCA) and his successors. *See Exec. Order No. 13526 § 3.1(b).* Thus, the accused lacked the authority to make classification decisions because he never occupied a position as an OCA. *See id.*

Moreover, allowing the accused, who was not an OCA at the time of the charged acts, to attack a classification decision with his personal opinion based on after-the-fact evidence undermines the entire classification system and should not be permitted.<sup>6</sup> *See Scarbeck v. United*

<sup>5</sup> Also under the Defense’s theory, the Government could prove its case with this irrelevant aggravating evidence, which is only appropriate for sentencing. *See United States v. Gogas*, 58 M.J. 96, 98 (C.A.A.F. 2003). Correspondingly, motive evidence is irrelevant to intent and inadmissible. *See United States v. Huet-Vaughn*, 43 M.J. 105, 113-114 (C.A.A.F. 1995). In particular, allowing the accused to present irrelevant evidence of motive would render the law moot, thereby allowing the accused to be judged not by the rule of law but by the end which his means were designed to serve. *See United States v. Cullen*, 454 F.2d 386, 392.

<sup>6</sup> The Government intends to file a motion at a later date to preclude challenges to propriety of classification. In *Scarbeck*, which involved the criminal prosecution of United States foreign service officer for communicating classified information to representatives of a foreign government, the Court of Appeals for the District of Columbia

*States*, 317 F.2d 546, 559-60 (D.C. Cir. 1962) (noting the absurdity of hypothetically allowing a government employee to challenge the classification decision of a superior in court) *cert. denied*, 374 U.S. 856 (1963). By alleging expertise, the Defense inappropriately attempts to justify the accused's criminal acts with irrelevant after-the-fact evidence. Any harm or its absence, which occurred after commission of the charged acts, had no bearing on the accused's intent at the time of committing the charged acts. See § II(a) *supra*. If some evidence raises an issue of mistake of fact where a knowledge of a particular fact is necessary to establish an offense, a mistake of fact defense must be instructed upon. See Benchbook (5-11). However, the mistake must be considered as it existed at the time of the offense and not with respect to after-the-fact evidence. See Benchbook (5-11-1).

Likewise, the alleged absence of harm is irrelevant to any impeachment of an OCA. At a minimum, courts grant great deference to classification decisions. See, e.g., *United States v. El-Mezain*, 664 F.3d 467, 523 (5th Cir. 2011) (declining to "second guess" the Government's determination of what is properly classified). Classification decisions contemplate only the data currently available for determinations of which information directly affects the national defense, thereby requiring classification protection. See *United States v. Dedeyan*, 584 F.2d 36, 41 (4th Cir. 1978) (discussing the necessity of classifying information as it currently bears on the national defense). Any speculation regarding *ex post* damage is irrelevant to classification decisions made *ex ante*. Events occurring after classification do not transform a proper classification decision into an improper one, nor has the Defense cited any authority to support its claim. Accordingly, harm and its absence are irrelevant to impeachment and should not be permitted.

After the Government, on direct, questions witnesses, including OCAs or senior officials on national defense information, which can include classification, the Defense can attack the process of classification. Also, the Defense may attack a witness's credibility in accordance with the Military Rules of Evidence, including for truthfulness and bias. See MRE 608. However, the Government does not need to prove actual harm and therefore will not raise the issue on direct examination.<sup>7</sup> Accordingly, any impeachment involving actual harm would be outside the scope and excludable. See MRE 611(b).

---

held that, under 50 U.S.C. § 783, the government was not required to establish the propriety of a classification determination, deciding that the executive's determination is not reviewable as part of the criminal prosecution. See *Scarbeck*, 317 F.2d at 557-60. Describing a challenge to the propriety of classification as absurd, the Court stated, "But certainly an employee of the State Department could not bring an action in the courts to remove the label 'Secret' attached by his superiors to a particular document, simply because he was being blackmailed and wished to be able to offer the document to his blackmailers without criminal consequences. Merely to describe such a litigation is enough to show its absurdity. Yet appellant is urging that after such an employee has obtained and delivered a classified document to an agent of a foreign power, knowing the document to be classified, he can present proof that his superior officer had no justification for classifying the document, and can obtain an instruction from the court to the jury that one of their duties is to determine whether the document, admittedly classified, was of such a nature that the superior was justified in classifying it. The trial of the employee would be converted into a trial of the superior." *Id.* at 559-60.

<sup>7</sup> This statement is premised on the exclusion of actual harm in accordance with this motion.

### III. DEFENSE'S GRIEVOUS BODILY HARM EXAMPLE DEMONSTRATES IRRELEVANCE OF ACTUAL HARM OR DAMAGE

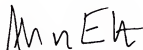
During the Article 39a on 26 April 2012, the Defense raised grievous bodily harm as an example to demonstrate the relevance of damage reports. The Defense stated, "To use an example, if we were to charge someone with grievous bodily harm—say, your act could cause grievous bodily harm. The medical report would obviously be relevant to that." Audio Record, Article 39a at 11:25:24–11:25:37 (26 April 2012). Under Article 128, UCMJ, the elements for assault with a dangerous weapon or other means or force likely to produce death or grievous bodily harm are:

- i) That the accused attempted to do, offered to do, or did bodily harm to a certain person;
- ii) That the accused did so with a certain weapon, means, or force;
- iii) That the attempt, offer, or bodily harm was done with unlawful force or violence; and
- iv) That the weapon, means, or force was used in a manner likely to produce death or grievous bodily harm

MCM pt. IV, ¶ 54.b.(4)(b); *United States v. Bean*, 62 M.J. 264, 266 (C.A.A.F. 2005). The Government does not dispute that a medical report could be relevant where the specification alleged actual bodily harm. However, in the case at bar, the Government does not need to prove harm or damage because neither harm nor damage has been alleged; neither is an element to any specification. See *Gorin* 312 U.S. at 29; Charge Sheet. Establishing the creation of the risk of substantial bodily injury does not require an actual injury. See *United States v. Rivera*, 54 M.J. 489, 492 (C.A.A.F. 2001). Moreover, any comparison of assault criminal law to a specification under the Espionage Act is inapposite because the Espionage Act is unique in criminal law. See *Schenck*, Edgar & Schmidt, *supra*. Nevertheless, actual harm or damage, or the lack thereof, is irrelevant under the Defense's hypothetical as applied to this case because harm is not an element.

### CONCLUSION

For the foregoing reasons, the Government respectfully requests that the Court grant this motion and preclude the defense from raising or eliciting any discussion, reference, or argument, to include the introduction of any documentary or testimonial evidence, relating to actual harm or damage, or lack thereof, from pretrial motions related to the merits portion of trial and from the merits portion of trial.



ALEXANDER S. VON ELTEN  
CPT, JA  
Assistant Trial Counsel



ASHDEN FEIN  
MAJ, JA  
Trial Counsel

Enclosure

I certify that I served or caused to be served a true copy of the above on Mr. David Coombs, Civilian Defense Counsel via electronic mail, on 21 June 2012.



ASHDEN FEIN  
MAJ, JA  
Trial Counsel





## INTERNAL SECURITY OF THE UNITED STATES

---

MAY 27 (legislative day, MAY 28), 1949.—Ordered to be printed

---

Mr. EASTLAND, from the Committee on the Judiciary, submitted the following

## REPORT

[To accompany S. 595]

The Committee on the Judiciary, to whom was referred the bill (S. 595) relating to the internal security of the United States, having considered the same, report favorably thereon with an amendment in the nature of a substitute, and recommend that the bill, as amended, do pass.

## AMENDMENT

Strike all after the enacting clause and insert the following:

That title 18, United States Code, section 793, be, and the same is hereby, amended to read as follows:

"(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, fueling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, or other place connected with the national defense owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers, departments, or agencies, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, or stored, under any contract or agreement with the United States, or any department or agency thereof, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place so designated by the President by proclamation in time of war or in case of national emergency in which anything for the use of the Army, Navy, or Air Force is being prepared or constructed or stored, information as to which prohibited place the President has determined would be prejudicial to the national defense; or

"(b) Whoever, for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or

"(c) Whoever, for the purpose aforesaid, receives or obtains or agrees or attempts to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this chapter; or

"(d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or

"(e) Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or

"(f) Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of his trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer—

"Shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

"(g) If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy."

SEC. 2. An indictment for any violation of title 18, United States Code, section 792, 793, or 794, may be found at any time within ten years next after such violation shall have been committed. This section shall not authorize prosecution, trial, or punishment for any offense now barred by the provisions of existing law.

SEC. 3. The Act of June 8, 1938 (52 Stat. 631; 22 U. S. C. 611-621), entitled "An Act to require the registration of certain persons employed by agencies to disseminate propaganda in the United States, and for other purposes", as amended, is hereby further amended as follows:

(a) Strike out the word "and" at the end of section 1 (c) (3), insert the word "and" at the end of section 1 (c) (4), and add the following subsection immediately after section 1 (c) (4):

"(5) any person who has knowledge of or has received instruction or assignment in the espionage, counterespionage, or sabotage service or tactics of a government of a foreign country or of a foreign political party, unless such knowledge, instruction, or assignment has been acquired by reason of civilian, military, or police service with the United States Government, the governments of the several States, their political subdivisions, the District of Columbia, the Territories, the Canal Zone, or the insular possessions, or unless such knowledge has been acquired solely by reason of academic or personal interest not under the supervision of or in preparation for service with the government of a foreign country or a foreign political party or

unless, by reason of employment at any time by an agency of the United States Government having responsibilities in the field of intelligence, such person has made full written disclosure of such knowledge or instruction to officials within such agency, such disclosure has been made a matter of record in the files of such agency, and a written determination has been made by the Attorney General or the Director of Central Intelligence that registration would not be in the interest of national security."

(b) Add the following subsection immediately after section 8 (d):

"8. (c) Failure to file any such registration statement or supplements thereto as is required by either section 2 (a) or section 2 (b) shall be considered a continuing offense for as long as such failure exists, notwithstanding any statute of limitation or other statute to the contrary."

Sec. 4. (a) Whoever willfully shall violate any such regulation or order as, pursuant to lawful authority, shall be or has been promulgated or approved by the Secretary of Defense, or by any military commander designated by the Secretary of Defense, for the protection or security of military or naval aircraft, airports, airport facilities, vessels, harbors, ports, piers, water-front facilities, bases, forts, posts, laboratories, stations, vehicles, equipment, explosives, or other property or places subject to the jurisdiction, administration, or in the custody of the National Military Establishment, any Department or agency of which said Establishment consists, or any officer or employee of said Establishment, Department or agency, relating to fire hazards, fire protection, lighting, machinery, guard service, disrepair, disuse or other unsatisfactory conditions thereon, or the ingress thereto or egress or removal of persons therefrom, or otherwise providing for safeguarding the same against destruction, loss, or injury by accident or by enemy action, sabotage or other subversive actions, shall be guilty of a misdemeanor and upon conviction thereof shall be liable to a fine of not to exceed \$5,000 or to imprisonment for not more than one year, or both.

(b) Every such regulation or order shall be posted in conspicuous and appropriate places.

(c) In time of war, or national emergency as proclaimed by the President, the provisions of this section may be extended by Presidential proclamation to include such property and places as the President may therein designate in the interest of national security.

(d) If any provision of this section or the application of such provision to any circumstance shall be held invalid, the validity of the remainder of this section and the application of such provision to other circumstances shall not be affected thereby.

#### PURPOSE OF AMENDMENT

In general, the purpose of the amendment is to make the bill, as introduced, conform to the concern of the sponsor and subcommittee about the deletion of certain subject matter and to the changes necessitated by the evidence brought out in the hearings. The quantum and complexity of the individual amendments warranted the entire rewriting of the legislation that it may be reported with one amendment in the nature of a substitute.

Specifically, the amendment accomplishes the following (taken in chronological order of sections and subsections):

##### *Section 1, subsection (a)*

The words "or Air Force" have been inserted following the words "Army or Navy" on line 17, page 2, of the bill as introduced. The purpose of this amendment is to include places in which anything is being prepared or constructed for the Air Force, as well as places in which anything is being prepared or constructed for the Army and Navy. The reason for this is that the Air Force has become a separate entity since the original enactment of the espionage statutes.

Following the word "which" found on page 2, line 18, of the bill as introduced there has been inserted the words "prohibited place". The purpose of this second amendment in subsection (a) is purely for clarity indicating to what the word "which" refers.

*Section 1, subsection (b)*

No change from the bill as introduced.

*Section 1, subsection (c)*

No change from the bill as introduced.

*Section 1, subsection (d)*

Following the word "which" found on page 3, line 17, of the bill as introduced there has been inserted the words "information the possessor has reason to believe". The purpose of this amendment is to require some degree of scienter in order to constitute a violation of the subsection insofar as the unlawful transmission of "information" is concerned.

Following the word "nation" found on page 3, line 19, of the bill as introduced there was deleted all down to and including the word "transmit" found on line 20 of the same page of the bill as introduced and was inserted in lieu thereof the following:

willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted.

The purpose of this amendment is to include the delivery, as well as communication or transmission of the items included in the subsection, and also to include those persons who would cause such communication, delivery, or transmission as well as those who actually communicate, deliver, or transmit such items.

*Section 1, subsection (e)*

The same amendment is made following the word "nation" on page 4, line 5, of the bill as introduced as made in the second amendment in section 1, subsection (d), immediately above.

*Section 1, subsection (f)*

Following the word "model" found on page 4, line 14, of the bill as introduced there has been inserted the words "instrument, appliance,". The purpose of this amendment is merely to add instruments and appliances among the items enumerated in the subsection.

On page 4, line 21, of the bill as introduced the word "actually" has been deleted. The purpose of this amendment is merely to eliminate the word "actually" as superfluous.

On page 4, line 22, of the bill as introduced the word "thereof" has been deleted, and there has been inserted in its place the words "of such loss, theft, abstraction, or destruction". The purpose of this amendment is merely for clarity and does not change the substance of the subsection.

*Section 1, subsection (g)*

On page 5, line 1, of the bill as introduced there has been deleted the word "the" and inserted in lieu thereof the words "any of the foregoing". The purpose of this amendment is merely for clarity and does not change the substance of the subsection.

Since the remaining sections of the bill as introduced and sections of the substitute amendment are not comparable because of considerable change in the sectional numeration, the following changes will be considered by page and line reference to the bill as introduced.

On page 5 of the bill as introduced, section 2 has been deleted *en toto*. The purpose of this amendment is to delete a section which appears superfluous, inasmuch as the prosecution of all Federal offenses is under the direction of the Attorney General.

On page 5, line 11, of the bill as introduced, the numeral "3" has been struck and the numeral "2" inserted in lieu thereof. The purpose of this amendment is merely to renumber the section.

On page 5, line 13, of the bill as introduced, the words "without regard to any statute of limitations." have been deleted, and there has been inserted in lieu thereof the words "within 10 years next after such violation shall have been committed." The purpose of this amendment is to provide a statute of limitations of 10 years with respect to the prosecution of espionage violations, rather than removing such violations from the statute of limitations entirely as originally proposed.

On page 5, line 17, of the bill as introduced, the numeral "4" has been struck and the numeral "3" inserted in lieu thereof. The purpose of this amendment is merely to renumber the section.

In addition to certain minor technical amendments, the following has been added to line 9, page 6, after changing the semicolon to a comma:

the governments of the several States, their political subdivisions, the District of Columbia, the Territories, the Canal Zone, and the insular possessions, or unless such knowledge has been acquired solely by reason of academic or personal interest not under the supervision of or in preparation for service with the government of a foreign country or a foreign political party

The purpose of this amendment is to include within the proviso or exception those enumerated therein in the belief that there should be no intention to include such parties nor would their inclusion contribute to the internal security of the country.

Following the word "party" in the amendment immediately above there has been added the additional words as follows:

or loss, by reason of employment at any time by an agency of the United States Government having responsibilities in the field of intelligence, such person has made full written disclosure of such knowledge or instruction to officials within such agency, such disclosure has been made a matter of record in the files of such agency, and a written determination has been made by the Attorney General or the Director of Central Intelligence that registration would not be in the interest of national security.

The purpose of this amendment is merely to add another category of persons who would not be required to register under the section.

On page 6, line 12, in the bill as introduced, there has been deleted everything after the word "file" down through and including the word "and" on line 13 and there has been inserted in lieu thereof the following: "any such registration statement or supplements thereto as is required by either section 2 (a) or." The purpose of this amendment is merely for clarity and does not change the substance of the section.

On page 6, line 17 of the bill as introduced, delete section 5 in toto. The wire-tapping provision has been stricken since the sponsor and your committee experienced concern both as to the advisability of enacting such a section and as to the propriety of joining it with amendments to the espionage laws. After some consultation it was decided to introduce a bill in the nature of a substitute which omitted wire-tapping and on which the hearings were held.

On page 8 of the bill as introduced, commencing with and including line 23, strike out the remainder of the bill and insert the following in lieu thereof:

SEC. 4. (a) Whoever willfully shall violate any such regulation or order as, pursuant to lawful authority, shall be or has been promulgated or approved by the Secretary of Defense, or by any military commander designated by the Secretary of Defense, for the protection or security of military or naval aircraft, airports, airport facilities, vessels, harbors, ports, piers, water-front facilities, bases, forts, posts, laboratories, stations, vehicles, equipment, explosives, or other property or places subject to the jurisdiction, administration, or in the custody of the National Military Establishment, any Department or agency of which said Establishment consists, or any officer or employee of said Establishment, Department, or agency, relating to fire hazards, fire protection, lighting, machinery, guard service, disrepair, disuse, or other unsatisfactory conditions thereon, or the ingress thereto or egress or removal of persons therefrom, or otherwise providing for safeguarding the same against destruction, loss, or injury by accident or by enemy action, sabotage or other subversive actions, shall be guilty of a misdemeanor and upon conviction thereof shall be liable to a fine of not to exceed \$5,000 or to imprisonment for not more than one year, or both.

(b) Every such regulation or order shall be posted in conspicuous and appropriate places.

(c) In time of war, or national emergency as proclaimed by the President, the provisions of this section may be extended by Presidential proclamation to include such property and places as the President may therein designate in the interest of national security.

(d) If any provision of this section or the application of such provision to any circumstance shall be held invalid, the validity of the remainder of this section and the application of such provision to other circumstances shall not be affected thereby.

The purpose of this amendment is to combine sections 6 and 7 of the bill as introduced into one section, covering the protection of both water and air facilities, rather than having a separate section for each facility. The amendment also makes it clear that, except in time of war or national emergency, the provisions of the section shall apply only to military property. Section 8 of the bill has been deleted as superfluous.

#### STATEMENT

The bill was introduced at the request of the Attorney General of the United States and has been drafted to carry out the recommendations of the Interdepartmental Intelligence Committee, composed of representatives of Military Intelligence and the Federal Bureau of Investigation of the Department of Justice. The recommendations reflect conclusions which were unanimously reached by the Interdepartmental Intelligence Committee, after a thorough study of the provisions and inadequacies of existing law, beginning in 1945, and are based on the needs and experiences of the investigative agencies during both World War II and peacetime.

The first section of the substitute amendment would amend the fourth paragraph of title 18, United States Code, section 793 (subsec. 1 (d) of the bill), to provide that only those who have lawful possession of the items relating to national defense enumerated therein shall be subject to its provisions. This is proposed in view of the fact that a refusal to deliver such items in response to a proper demand therefor is an element of an offense under existing law, whereas it is deemed advisable that those who have unauthorized possession of such items should be subject to the provisions of a



separate subsection, as hereinafter explained, and required to surrender them to the proper authorities regardless of the demand therefor.

The first section of the substitute amendment would also amend the fourth paragraph of title 18, United States Code, section 793 (subsec. 1 (d) of the bill) to include "information relating to the national defense, which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation" among the items of which the unauthorized transmission or retention would be unlawful. The phrase "which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation" would modify only "information relating to the national defense" and not the other items enumerated in the subsection. It is deemed advisable to broaden the subsection to include such information, in order to render the law more effective against unauthorized transmissions and retentions which may not come within the existing specifically enumerated items but which are considered nonetheless dangerous to the national security.

The first section of the substitute amendment would amend title 18, United States Code, section 793, to provide (subsec. 1 (e) of the bill) that those who have unauthorized possession of the items enumerated therein must surrender possession thereof to the proper authorities regardless of a demand therefor. Existing law provides no penalty for the unauthorized possession of such items unless a demand for them is made by the person entitled to receive them. The dangers surrounding the unauthorized possession of the items enumerated in this statute are self-evident, and it is deemed advisable to require their surrender in such a case, regardless of demand, especially since their unauthorized possession may be unknown to the authorities who would otherwise make the demand. In summary, the only difference between subsection 1 (d) and subsection 1 (e) of title 18, United States Code, section 793, if amended as indicated, would be that a demand by the person entitled to receive the items would be a necessary element of an offense under subsection 1 (d) where the possession is lawful, whereas such a demand would not be a necessary element of an offense under subsection 1 (e) where the possession is unauthorized.

The first section of the substitute amendment would amend title 18, United States Code, section 793, by adding a provision (subsec. 1 (f) (2)) to provide for the punishment of those who are entrusted with the items relating to national defense enumerated therein and who have knowledge of, but fail to report, the loss, theft, abstraction, destruction, or unlawful transmission of such items. The danger of such an item, e. g., a code book or plan of operation, being lost, stolen, or compromised by the enemy or prospective enemy, needs no emphasis. As an illustration, it is now common knowledge that our compromise of an enemy coding system was an important factor in our defense and operations against the enemy in the early and vital stages of World War II. It is not unreasonable to assume that the advantage would be reversed should an enemy compromise a coding system of the United States. The existing law provides no penalty for the failure to report such knowledge by those entrusted with the above items.

The first section of the substitute amendment (subsec. 1 (g)) would amend title 18, United States Code, section 793, to provide a penalty, identical to the penalty provided for a conspiracy to violate section 794, for a conspiracy to violate section 793. There appears to be no reason why a conspiracy to violate section 793 should not be similarly punishable as a conspiracy to violate section 794.

The first section of the substitute amendment would designate the several paragraphs of title 18, United States Code, section 793, as subsections "(a)" through "(g)" for purposes of convenient reference.

Section 2 of the substitute amendment would provide that an indictment for the violation of section 792, 793, or 794 of title 18, United States Code, could be found within 10 years after the commission of such violation. Under existing law (18 U. S. C. 3282), the statute of limitations with respect to a violation of section 792, 793, or 794 in peacetime is only 3 years. A violation of section 794 during war constitutes a capital offense and is therefore not subject to the statute of limitations (18 U. S. C. 3282). In view of the fact that a violation of section 792, 793, or 794 during either peace or war may not be detected, or the identity of the violator discovered, until more than 3 years after the violation was committed, e. g., until hostilities cease and the records of the enemy are accessible, it is considered advisable to amend the existing law so that the prosecution of an espionage violation may be instituted within 10 years after the commission of the violation. Such an amendment would also permit the prosecution and consequent public disclosures of such offenses to be held in abeyance, for strategical purposes, pending the detection and apprehension of other offenders who may also be involved in the same or affiliated espionage ring. The amendment, of course, because of the constitutional bar against ex post facto criminal laws, would not authorize the prosecution or punishment of an offense which is already barred by existing law.

Section 3 (a) of the substitute amendment would amend the Foreign Agents Registration Act of June 8, 1938, as amended (22 U. S. C. 611-621), by adding a subsection 1 (c) (5) immediately after subsection 1 (c) (4) (22 U. S. C. 611 (c) (4)) to require the registration of persons who have knowledge of, or have received instruction or assignment in, the espionage, counterespionage, or sabotage service or tactics of a foreign government or a foreign political party, unless such knowledge or instruction has been acquired by reason of civilian, military, or police service with the United States Government or the governments of the several States, or unless such knowledge has been acquired solely by reason of academic or personal interest not under the supervision of, or in preparation for, service with the government of a foreign country or a foreign political party, or unless, by reason of employment by an intelligence agency of the United States Government, such person has made full disclosure of such knowledge or instruction to officials within such agency.

Under existing law, a person trained by a foreign government for purposes of espionage or sabotage is immune to prosecution provided there is no substantial evidence of his having violated the espionage laws, and he is in no way obliged to divulge either his intentions or the very useful information which is peculiarly within his knowledge, information which if acquired by our counterintelligence agencies could spell the difference between success and catastrophe in counter-



acting the plans and tactics of an enemy. Examples of those who would come within this category are those whose operations may defy detection and those who may be dispatched to this country for purposes of espionage or sabotage and who either postpone their operations until an opportune time or, for fear of apprehension or other reason, abandoned their mission. The amendment would serve a threefold purpose, namely, to discourage further the unknown presence of potential spies and saboteurs; to provide a basis for the prosecution of unregistered potential spies and saboteurs before they commit an act of espionage or sabotage; and to assist this Government in its counterintelligence work by acquiring the information regarding foreign espionage and sabotage systems and tactics that would be disclosed by those who elected to register rather than run the risk of prosecution for not so registering.

Section 3 (b) of the substitute amendment would amend the Foreign Agents Registration Act by adding the subsection 8 (e) immediately after subsection 8 (d) (22 U. S. C. 618 (d)) to provide that a failure to file a registration statement or supplements thereto as required by sections 2 (a) or 2 (b) (22 U. S. C. 612 (a) (b)) shall be considered a continuing offense for as long as such failure exists, notwithstanding any statute of limitations or other statute to the contrary. The purpose of this subsection is to permit the prosecution of an offender at any time during the period he continues to disregard the statute and not merely within a 3-year period from the time that he first became subject to the law and should have registered but failed to do so.

Section 4 of the substitute amendment would provide a maximum penalty of a \$5,000 fine and 1 year imprisonment for the willful violation of regulations or orders promulgated by the Secretary of Defense respecting the protection of military property. A similar law, respecting the protection of vessels and waterfront facilities, approved July 9 1943 (50 App. U. S. C. 1312), existed during World War II, but expired by reason of its own provision on June 30, 1947. The section is deemed advisable in order to provide protection for military property from both accidental and deliberate danger. The section would also provide that in time of war, or national emergency as proclaimed by the President, the provisions may be extended by Presidential proclamation to include such property and places as the President may designate in the interest of national security.

The entire bill as amended by your committee has been drafted to serve the needs of the departments of Justice, the Army, the Air Force, and the Navy in the successful discharge of their responsibility to protect and improve the internal security of the Nation. The swift and more devastating weapons of modern warfare, coupled with the treacherous operations of those who would weaken our country internally, preliminary to and in conjunction with external attack, have made it imperative that we strengthen and maintain an alert and effective vigilance.

O

UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

**GOVERNMENT PROPOSED  
MEMBER INSTRUCTIONS**

22 June 2012

**RELIEF SOUGHT**

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court adopt the Government's proposed member instructions for all charged offenses and lesser-included offenses.

**BURDEN OF PERSUASION AND BURDEN OF PROOF**

As the moving party, the United States has the burden of persuasion on any factual issue the resolution of which is necessary to decide the motion. *Manual for Courts-Martial (MCM)*, *United States*, Rule for Courts-Martial (RCM) 905(c)(2) (2008). The burden of proof is by a preponderance of the evidence. RCM 905(c)(1).

**FACTS**

The accused is charged with giving intelligence to the enemy, in violation of Article 104, Uniform Code of Military Justice (UCMJ). The accused is also charged with eight specifications alleging misconduct in violation of 18 U.S.C. § 793(e), five specifications alleging misconduct in violation of 18 U.S.C. § 641, two specifications alleging misconduct in violation of 18 U.S.C. § 1030(a)(1), five specifications alleging misconduct in violation of Article 92, UCMJ, and one specification alleging misconduct prejudicial to good order and discipline and service discrediting.

**WITNESSES/EVIDENCE**

The United States requests this Court consider the referred charge sheet in support of its motion, as well as Enclosures 1-7. Other than the transcript at Enclosure 1, the United States was unable to obtain the transcripts for the other cases identified by the Court in the last Article 39(a) session.

## **PROPOSED INSTRUCTIONS**

### **The Specification of Charge I: Violation of the UCMJ, Article 104<sup>1</sup>**

In the Specification of Charge I, the accused is charged with Aiding the Enemy by Giving Intelligence, in violation of Article 104, UCMJ. To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

- (1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 1 November 2009 and on or about 27 May 2010, the accused, without proper authority, knowingly gave intelligence information to al-Qaeda or [classified enemy];
- (2) That the accused did so through indirect means;
- (3) That al-Qaeda or [classified enemy] was an enemy; and
- (4) That this intelligence information was true, at least in part.

Adapted from *Benchbook*, paragraphs 2-5-9 and 3-28-4.

#### **Proposed Instruction No. 1**

"Intelligence" means any helpful information, given to and received by the enemy, which is true, at least in part.

*Benchbook*, paragraph 3-28-4.

#### **Proposed Instruction No. 2**

"Enemy" includes organized opposing forces in time of war, any other hostile body that our forces may be opposing, such as a rebellious mob or a band of renegades, and includes civilians as well as members of military organizations. "Enemy" is not restricted to the enemy government or its armed forces. All the citizens of one belligerent are enemies of the government and all the citizens of the other.

*Benchbook*, paragraph 3-28-4.

#### **Proposed Instruction No. 3**

---

<sup>1</sup> The Court ruled that it would adopt the instructions for Article 104(2), Giving Intelligence to the Enemy, found in *U.S. Department of the Army, Pam. 27-9, Military Judges' Benchbook* (1 January 2010) (*Benchbook*). See Appellate Exhibit LXXXI. Proposed Instructions 1 and 2 are from the *Benchbook*; instructions 3 and 4 are the Court's proposed instructions for "knowledge" and "indirect means." The Court invited the parties to propose different instructions. *Id.*

"Knowingly" means Giving Intelligence to the Enemy under Article 104(2) requires actual knowledge by the accused that he was giving intelligence to the enemy. This is true whether the giving of intelligence is by direct or indirect means. A person cannot violate Article 104 by acting inadvertently, accidentally, or negligently.

See *MCM*, pt. IV, ¶ 28c(5)(c); *United States v. Olson*, 20 C.M.R. 461 (A.B.R. 1955); Appellate Exhibit LXXXI.

#### Proposed Instruction No. 4

"Indirect means" means that the accused knowingly gave the intelligence to the enemy through a third party or in some other indirect way. The accused must actually know that by giving the intelligence to the third party that he was giving intelligence to the enemy through this indirect means.

Appellate Exhibit LXXXI.

#### **Specification 1 of Charge II: Violation of the UCMJ, Article 134<sup>2</sup>**

In Specification 1 of Charge II, the accused is charged with wrongfully and wantonly causing intelligence to be published on the internet. To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 1 November 2009 and on or about 27 May 2010, the accused did wrongfully and wantonly cause to be published on the internet intelligence belonging to the United States government, having knowledge that intelligence published on the internet is accessible to the enemy; and

(2) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchbook*, paragraph 2-5-9.

#### Proposed Instruction No. 1

"Conduct prejudicial to good order and discipline" is conduct which causes a reasonably direct and obvious injury to good order and discipline. "Service discrediting conduct" is conduct which tends to harm the reputation of the service or lower it in public esteem.

*Benchbook*, paragraph 3-60-2A.

#### Proposed Instruction No. 2

---

<sup>2</sup> Proposed Instructions 1 and 2 should be given for all 16 specifications of Charge II, as each specification alleges conduct prejudicial to good order and discipline and service discrediting.

With respect to “prejudice to good order and discipline,” the law recognizes that almost any irregular or improper act on the part of a service member could be regarded as prejudicial in some indirect or remote sense; however, the only acts punishable under the Article are those acts where the prejudice is reasonably direct and palpable.

With respect to “service discrediting,” the law recognizes that almost any irregular or improper act on the part of a service member could be regarded as service discrediting in some indirect or remote sense; however, only those acts which would have a tendency to bring the service into disrepute or which tend to lower it in public esteem are punishable under this Article.

*Benchbook*, paragraph 3-60-2A.

#### Proposed Instruction No. 3

“Wrongfully” means without legal justification or excuse.

*Benchbook*, paragraph 3-60-2A, NOTE 3.

#### Proposed Instruction No. 4

“Wanton” means a degree of carelessness greater than simple negligence. “Simple negligence” is the absence of due care; that is, an act by a person who is under a duty to use due care which demonstrates a lack of care for the safety of others which a reasonably careful person would have used under the same or similar circumstances. “Wantonness,” on the other hand, is a negligent act combined with a gross or deliberate disregard for the foreseeable results to others. “Wanton” is akin to reckless.

Adapted from *Benchbook*, paragraph 3-35-1, NOTE 10.

#### Proposed Instruction No. 5

“Intelligence” is information that may be useful to the enemy for any of the many reasons that make information valuable to belligerents. Intelligence imports that the information conveyed is true or implies the truth, at least in part.

See Appellate Exhibit LXXX; *MCM*, pt. IV, ¶ 28c(5).

#### Proposed Instruction No. 6

“Enemy” includes organized opposing forces in time of war, any other hostile body that our forces may be opposing, such as a rebellious mob or a band of renegades, and includes civilians as well as members of military organizations. “Enemy” is not restricted to the enemy government or its armed forces. All the citizens of one belligerent are enemies of the government and all the citizens of the other.

*Benchbook*, paragraph 3-28-4.

### Proposed Instruction No. 7

I have instructed you that you must be satisfied beyond a reasonable doubt that the accused knew that intelligence published on the internet was accessible to the enemy. This knowledge, like any other fact, may be proved by circumstantial evidence. In deciding this issue you must consider all relevant facts and circumstances, including, but not limited to, the accused's training, experience, and military occupational specialty.

Adapted from *Benchbook*, paragraph 7-3, NOTE 3.

### **Specification 2 of Charge II: Violation of the UCMJ, Article 134<sup>3</sup>**

In Specification 2 of Charge II, the accused is charged with transmitting a video file named "12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.avi" to a person not entitled to receive it, in violation of 18 U.S.C. § 793(e). To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 15 February 2010 and on or about 5 April 2010, the accused had possession of information relating to the national defense, to wit: a video file named "12 JUL 07 CZ ENGAGEMENT ZONE 30 GC Anyone.avi";

(2) That the possession was unauthorized;

(3) That the accused had reason to believe that such information could be used to the injury of the United States or to the advantage of any foreign nation;

(4) That the accused willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, the said information, to a person not entitled to receive it;

(5) That, at the time, 18 U.S.C. § 793(e) was in existence; and

(6) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchbook*, paragraph 2-5-9; 18 U.S.C. § 793(e).

### Proposed Instruction No. 1

---

<sup>3</sup> The United States requests that Proposed Instructions 1-11 be given for each specification alleging misconduct in violation of 18 U.S.C. § 793(e).

Title 18, United States Code, Section 793(e), makes it a crime to disclose or transmit information relating to the national defense to unauthorized persons.

#### Proposed Instruction No. 2

The word “possession” is a commonly used and commonly understood word. To “possess” means to exercise control of something. Possession may be direct physical custody, like holding an item in one’s hand, or it may be constructive, as in the case of a person who hides an item in a locker or car to which that person may return to retrieve it. Possession inherently includes the power or authority to preclude control by others. It is possible, however, for more than one person to possess an item simultaneously, as when several people share control of an item.

*Benchbook*, paragraph 3-37-1.

#### Proposed Instruction No. 3

An individual has unauthorized possession of documents, photographs, videos, or computer files when he possesses such information under circumstances or in a location which is contrary to law or regulation for the conditions of his employment. In other words, the individual has unauthorized possession of the information when they move the information from official premises without proper authorization.

Adapted from *United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988) (Enclosure 1 at 194).

#### Proposed Instruction No. 4

The term “national defense” is a broad term which refers to the United States military and naval establishments and to all related activities of national preparedness, and includes all matters that may directly or may reasonably be connected with the defense of the United States against any of its enemies.

Adapted from *Gorin v. United States*, 312 U.S. 19 (1941); *United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988) (Enclosure 1 at 195); *United States v. Diaz*, 69 M.J. 127 (C.A.A.F. 2010) (Enclosure 2 at 4); *United States v. Regan* (Enclosure 7 at 18).

#### Proposed Instruction No. 5

To prove that documents, writings, photographs, videos, or information relate to the national defense, there are two things that the government must prove. First, it must prove that the disclosure of the material would be potentially damaging to the United States or might be useful to an enemy of the United States. Second, it must prove that the material is closely held by the United States government, in that the relevant government agency has sought to keep the information from the public generally, and the documents, photographs, videos, or computer files have not been made public and are not available to the general public. Where the information has been made public by the United States government and is found in sources lawfully available to the general public, it does not relate to the national defense. Similarly, where the sources of

information are lawfully available to the public, and the United States government has made no effort to guard such information, the information itself does not relate to the national defense.

Adapted from *United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988) (Enclosure 1 at 195-96); *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Dedeyan*, 584 F.2d 36 (4th Cir. 1978); *United States v. Squillacote*, 221 F.3d 542 (4th Cir. 2000); *United States v. Regan* (Enclosure 7 at 18-19)

#### Proposed Instruction No. 6

In determining whether material is “closely held,” you may consider whether it has been classified by appropriate authorities and whether it remained classified on the date or dates pertinent to the charge sheet. You may consider whether the information was classified or not in determining whether the information relates to the national defense. However, the fact that the information is designated as classified does not, in and of itself, demonstrate that the information relates to the national defense.

Adapted from *United States v. Regan* (Enclosure 7 at 19-20); *see also United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988) (Enclosure 1 at 196).

#### Proposed Instruction No. 7

“Reason to believe” means that the accused knew facts from which he concluded or reasonably should have concluded that the information could be used for the prohibited purposes. In considering whether the accused had reason to believe that the information could be used to the injury of the United States or to the advantage of a foreign country, you may consider the nature of the information involved. You need not determine that the accused had reason to believe that the information would be used against the United States, only that it could be so used.

*United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Diaz*, 69 M.J. 127 (C.A.A.F. 2010) (Enclosure 2 at 5); *United States v. Regan* (Enclosure 7 at 17-18); *see also* Mod. Fed. Jury Instr. (Enclosure 6) (citing *Truong*).

#### Proposed Instruction No. 8

The government does not have to prove that the accused had reason to believe that his act could both injure the United States and be to the advantage of a foreign country – the statute reads in the alternative. Also, the country to whose advantage the information could be used need not necessarily be an enemy of the United States. The statute does not distinguish between friend and enemy.

*United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Diaz*, 69 M.J. 127 (C.A.A.F. 2010) (Enclosure 2 at 5-6); *United States v. Regan* (Enclosure 7 at 17-18); *see also* Mod. Fed. Jury Instr. (Enclosure 6) (citing *Truong*).



#### Proposed Instruction No. 9

An act is done “willfully” if it is done voluntarily and intentionally and with the specific intent to do something that the law forbids; that is, with a bad purpose either to disobey or to disregard the law.

*United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988) (Enclosure 1 at 199); *United States v. Diaz*, 69 M.J. 127 (C.A.A.F. 2010) (Enclosure 2 at 6); *see also* Mod. Fed. Jury Instr. (Enclosure 6).

#### Proposed Instruction No. 10

In determining whether the person who received the information was entitled to have it, you may consider all the evidence introduced at trial, including any evidence concerning the classification status of the information, any evidence relating to law and regulations governing the classification and declassification of national security information, its handling, use, and distribution, as well as any evidence relating to regulations governing the handling, use, and distribution of information obtained from classified systems.

Adapted from *United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988); *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Diaz*, 69 M.J. 127 (C.A.A.F. 2010) (Enclosure 2 at 6); *see also* Mod. Fed. Jury Instr. (Enclosure 6).

#### Proposed Instruction No. 11

I have taken judicial notice that Title 18, United States Code Section 793(e) was in existence on the date alleged in the specification.<sup>4</sup>

#### **Specification 3 of Charge II: Violation of the UCMJ, Article 134**

In Specification 3 of Charge II, the accused is charged with transmitting more than one classified memorandum produced by a United States government intelligence agency to a person not entitled to receive them, in violation of 18 U.S.C. § 793(e). To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 22 March 2010 and on or about 26 March 2010, the accused had possession of information relating to the national defense, to wit: more than one classified memorandum produced by a United States government intelligence agency;

(2) That the possession was unauthorized;

---

<sup>4</sup> This assumes the Court takes judicial notice of the statute at a future motions hearing.

(3) That the accused had reason to believe that such information could be used to the injury of the United States or to the advantage of any foreign nation;

(4) That the accused willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, the said information, to a person not entitled to receive it;

(5) That, at the time, 18 U.S.C. § 793(e) was in existence; and

(6) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchbook*, paragraph 2-5-9; 18 U.S.C. § 793(e).

#### **Specification 4 of Charge II: Violation of the UCMJ, Article 134<sup>5</sup>**

In Specification 4 of Charge II, the accused is charged with stealing or converting the Combined Information Data Network Exchange Iraq database containing more than 380,000 records belonging to the United States government, of a value of more than \$1,000, in violation of 18 U.S.C. § 641. To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 5 January 2010, the accused did knowingly and willfully<sup>6</sup> steal, purloin, or convert to his use or the use of another a record or thing of value, to wit: the Combined Information Data Network Exchange Iraq database containing more than 380,000 records;

(2) That the CIDNE-I database belonged to the United States government or a department or agency thereof;

(3) That the CIDNE-I database was of a value of more than \$1,000;

(4) That the taking by the accused was with the intent to deprive the United States government of the use or benefit of the property;

(5) That, at the time, 18 U.S.C. § 641 was in existence; and

---

<sup>5</sup> The United States requests that Proposed Instructions I-9 be given for each offense alleging misconduct in violation of 18 U.S.C. § 641.

<sup>6</sup> Case law indicates that the accused must act "knowingly and willfully" under § 641, although the statute itself and most model instructions are not clear on this point. See *United States v. McGahee*, 257 F.3d 520, 531 (6th Cir. 2001) (instructing on "knowingly" and "willfully"); *United States v. Fowler*, 932 F. 2d 306, 316-17 (4th Cir. 1991) (instructing on "knowingly" and "willfully"); *United States v. Morison* (Enclosure 1 at 197); see also *United States v. Morissette*, 342 U.S. 246, 263 (1952) (holding that criminal intent is an essential element of 18 U.S.C. § 641). The Eight Circuit instructions helpfully incorporate the "knowingly and willfully" standard. See Enclosure 3.

(6) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchbook*, paragraph 2-5-9; 18 U.S.C. § 641; Model Crim. Jury Instr. 8th Cir. 6.18.641 (2011) (Enclosure 3).

#### Lesser-Included Offense

The offense of stealing or converting the CIDNE-I database, of a value of less than \$1,000, is a lesser-included offense of the offense set forth in Specification 4 of Charge II. When you vote, if you find the accused not guilty of the offense charged, that is, stealing or converting the CIDNE-I database, of a value of more than \$1,000, then you should consider the lesser-included offense of stealing or converting the CIDNE-I database, of a value of less than \$1,000, in violation of 18 U.S.C. § 641. To find the accused guilty of this lesser offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of all of the elements of the greater offense, except for the value element. The offense charged, and the lesser-included offense of stealing or converting the CIDNE-I database, of a value of less than \$1,000, differ in that the greater offense requires you to be satisfied beyond a reasonable doubt that the CIDNE-I database is worth more than \$1,000.

Adapted from *Benchbook*, paragraph 2-5-10.

#### Proposed Instruction No. 1

Title 18, United States Code, Section 641, makes it a crime for anyone to steal or knowingly convert any money or other property belonging to the United States having a value of more than \$1,000.

Pattern Crim. Jury Instr. 5th Cir. 2.33 (2001) (Enclosure 4).

#### Proposed Instruction No. 2

The word "value" means the face, par, or market value, or cost price, either wholesale or retail, whichever is greater.

18 U.S.C. § 641; Pattern Crim. Jury Instr. 5th Cir. 2.33 (2001) (Enclosure 4).

#### Proposed Instruction No. 3

The market value of stolen goods may be determined by reference to a price that is commanded in the market place, whether that market place is legal or illegal. In other words, market value is measured by the price a willing buyer will pay a willing seller. The illegal market place is also known as a "thieves market."

Adapted from *United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988) (Enclosure 1 at 199); see *United States v. Oberhardt*, 887 F.2d 790 (7th Cir. 1989); *United States v. DiGilio*, 538 F.2d 972 (3d Cir. 1976).

#### Proposed Instruction No. 4

To “steal” or “convert” means the wrongful taking of property belonging to another with intent to deprive the owner of its use or benefit, either temporarily or permanently. Any appreciable change of the location of the property with the intent to deprive constitutes a stealing whether or not there is an actual removal of it from the owner’s premises.

Pattern Crim. Jury Instr. 5th Cir. 2.33 (2001) (Enclosure 4); *United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988) (Enclosure 1 at 197-98).

#### Proposed Instruction No. 5

No particular type of movement or carrying away is required to constitute a “taking.” Thus, one may convert property of the United States without intending to permanently deprive the United States of that property.

Pattern Crim. Jury Instr. 5th Cir. 2.33 (2001) (Enclosure 4); *United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988) (Enclosure 1 at 198).

#### Proposed Instruction No. 6

It is not necessary to prove that the accused knew that the United States government owned the property at the time of the wrongful taking.

Pattern Crim. Jury Instr. 5th Cir. 2.33 (2001) (Enclosure 4); Model Crim. Jury Instr. 8th Cir. 6.18.641 (2011) (Enclosure 3).

#### Proposed Instruction No. 7

Governmental information, including classified information, although intangible, is a species of property and a thing of value.

*United States v. Fowler*, 932 F.2d 306 (4th Cir. 1991); *United States v. Jeter*, 775 F.2d 670 (6th Cir. 1985); *United States v. Girard*, 601 F.2d 69 (2d Cir. 1979).

#### Proposed Instruction No. 8

An act is done “willfully” if it is done voluntarily and intentionally and with the specific intent to do something the law forbids; that is, with a bad purpose to disobey or disregard the law. An act is done “knowingly” if it is done voluntarily and intentionally and not because of mistake or accident or other innocent reason.

*United States v. Fowler*, 932 F.2d 306 (4th Cir. 1991); *United States v. McGahee*, 257 F.3d 520 (6th Cir. 2001).

Proposed Instruction No. 9

I have taken judicial notice that Title 18, United States Code Section 641 was in existence on the date alleged in the specification.<sup>7</sup>

**Specification 5 of Charge II: Violation of the UCMJ, Article 134**

In Specification 5 of Charge II, the accused is charged with transmitting more than twenty classified records from the Combined Information Data Network Exchange Iraq database to a person not entitled to receive them, in violation of 18 U.S.C. § 793(e). To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 9 February 2010, the accused had possession of information relating to the national defense, to wit: more than twenty classified records from the Combined Information Data Network Exchange Iraq database;

(2) That the possession was unauthorized;

(3) That the accused had reason to believe that such information could be used to the injury of the United States or to the advantage of any foreign nation;

(4) That the accused willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, the said information, to a person not entitled to receive it;

(5) That, at the time, 18 U.S.C. § 793(e) was in existence; and

(6) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchbook*, paragraph 2-5-9; 18 U.S.C. § 793(e).

**Specification 6 of Charge II: Violation of the UCMJ, Article 134**

In Specification 6 of Charge II, the accused is charged with stealing or converting the Combined Information Data Network Exchange Afghanistan database containing more than 90,000 records belonging to the United States government, of a value of more than \$1,000, in violation of 18 U.S.C. § 641. To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

---

<sup>7</sup> This assumes the Court takes judicial notice of the statute at a future motions hearing.

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 8 January 2010, the accused did knowingly and willfully steal, purloin, or convert to his use or the use of another a record or thing of value, to wit: the Combined Information Data Network Exchange Afghanistan database containing more than 90,000 records;

(2) That the CIDNE-A database belonged to the United States government or a department or agency thereof;

(3) That the CIDNE-A database was of a value of more than \$1,000;

(4) That the taking by the accused was with the intent to deprive the United States government of the use or benefit of the property;

(5) That, at the time, 18 U.S.C. § 641 was in existence; and

(6) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchbook*, paragraph 2-5-9; 18 U.S.C. § 641; Model Crim. Jury Instr. 8th Cir. 6.18.641 (2011) (Enclosure 3).

#### Lesser-Included Offense

The offense of stealing or converting the CIDNE-A database, of a value of less than \$1,000, is a lesser-included offense of the offense set forth in Specification 6 of Charge II. When you vote, if you find the accused not guilty of the offense charged, that is, stealing or converting the CIDNE-A database, of a value of more than \$1,000, then you should consider the lesser-included offense of stealing or converting the CIDNE-A database, of a value of less than \$1,000, in violation of 18 U.S.C. § 641. To find the accused guilty of this lesser offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of all of the elements of the greater offense, except for the value element. The offense charged, and the lesser-included offense of stealing or converting the CIDNE-A database, of a value of less than \$1,000, differ in that the greater offense requires you to be satisfied beyond a reasonable doubt that the CIDNE-A database is worth more than \$1,000.

Adapted from *Benchbook*, paragraph 2-5-10.

#### **Specification 7 of Charge II: Violation of the UCMJ, Article 134**

In Specification 7 of Charge II, the accused is charged with transmitting more than twenty classified records from the Combined Information Data Network Exchange Afghanistan database to a person not entitled to receive them, in violation of 18 U.S.C. § 793(e). To find the accused

guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 31 December 2009 and on or about 9 February 2010, the accused had possession of information relating to the national defense, to wit: more than twenty classified records from the Combined Information Data Network Exchange Afghanistan database;

(2) That the possession was unauthorized;

(3) That the accused had reason to believe that such information could be used to the injury of the United States or to the advantage of any foreign nation;

(4) That the accused willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, the said information, to a person not entitled to receive it;

(5) That, at the time, 18 U.S.C. § 793(e) was in existence; and

(6) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchbook*, paragraph 2-5-9; 18 U.S.C. § 793(e).

#### **Specification 8 of Charge II: Violation of the UCMJ, Article 134**

In Specification 8 of Charge II, the accused is charged with stealing or converting a United States Southern Command database containing more than 700 records belonging to the United States government, of a value of more than \$1,000, in violation of 18 U.S.C. § 641. To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, on or about 8 March 2010, the accused did knowingly and willfully steal, purloin, or convert to his use or the use of another a record or thing of value, to wit: a United States Southern Command database containing more than 700 records;

(2) That the SOUTHCOM database belonged to the United States government or a department or agency thereof;

(3) That the SOUTHCOM database was of a value of more than \$1,000;

(4) That the taking by the accused was with the intent to deprive the United States government of the use or benefit of the property;

(5) That, at the time, 18 U.S.C. § 641 was in existence; and

(6) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchbook*, paragraph 2-5-9; 18 U.S.C. § 641; Model Crim. Jury Instr. 8th Cir. 6.18.641 (2011) (Enclosure 3).

#### Lesser-Included Offense

The offense of stealing or converting the SOUTHCOM database, of a value of less than \$1,000, is a lesser-included offense of the offense set forth in Specification 8 of Charge II. When you vote, if you find the accused not guilty of the offense charged, that is, stealing or converting the SOUTHCOM database, of a value of more than \$1,000, then you should consider the lesser-included offense of stealing or converting the SOUTHCOM database, of a value of less than \$1,000, in violation of 18 U.S.C. § 641. To find the accused guilty of this lesser offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of all of the elements of the greater offense, except for the value element. The offense charged, and the lesser-included offense of stealing or converting the SOUTHCOM database, of a value of less than \$1,000, differ in that the greater offense requires you to be satisfied beyond a reasonable doubt that the SOUTHCOM database is worth more than \$1,000.

Adapted from *Benchbook*, paragraph 2-5-10.

#### **Specification 9 of Charge II: Violation of the UCMJ, Article 134**

In Specification 9 of Charge II, the accused is charged with transmitting more than three classified records from a United States Southern Command database to a person not entitled to receive them, in violation of 18 U.S.C. § 793(e). To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 8 March 2010 and on or about 27 May 2010, the accused had possession of information relating to the national defense, to wit: more than three classified records from a United States Southern Command database;

(2) That the possession was unauthorized;

(3) That the accused had reason to believe that such information could be used to the injury of the United States or to the advantage of any foreign nation;

(4) That the accused willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, the said information, to a person not entitled to receive it;



(5) That, at the time, 18 U.S.C. § 793(e) was in existence; and

(6) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchbook*, paragraph 2-5-9; 18 U.S.C. § 793(e).

#### **Specification 10 of Charge II: Violation of the UCMJ, Article 134**

In Specification 10 of Charge II, the accused is charged with transmitting more than five classified records relating to a military operation in Farah Province, Afghanistan occurring on or about 4 May 2009 to a person not entitled to receive them, in violation of 18 U.S.C. § 793(e). To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 11 April 2010 and on or about 27 May 2010, the accused had possession of information relating to the national defense, to wit: more than five classified records relating to a military operation in Farah Province, Afghanistan occurring on or about 4 May 2009;

(2) That the possession was unauthorized;

(3) That the accused had reason to believe that such information could be used to the injury of the United States or to the advantage of any foreign nation;

(4) That the accused willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, the said information, to a person not entitled to receive it;

(5) That, at the time, 18 U.S.C. § 793(e) was in existence; and

(6) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchbook*, paragraph 2-5-9; 18 U.S.C. § 793(e).

#### **Specification 11 of Charge II: Violation of the UCMJ, Article 134**

In Specification 11 of Charge II, the accused is charged with transmitting a file named "BE22 PAX.zip" containing a video named "BE22 PAX.wmv" to a person not entitled to receive it, in violation of 18 U.S.C. § 793(e). To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 1 November 2009 and on or about 8 January 2010, the accused had possession of information relating to the national defense, to wit: a file named "BE22 PAX.zip" containing a video named "BE22 PAX.wmv";

(2) That the possession was unauthorized;

(3) That the accused had reason to believe that such information could be used to the injury of the United States or to the advantage of any foreign nation;

(4) That the accused willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, the said information, to a person not entitled to receive it;

(5) That, at the time, 18 U.S.C. § 793(e) was in existence; and

(6) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchmark*, paragraph 2-5-9; 18 U.S.C. § 793(e).

#### **Specification 12 of Charge II: Violation of the UCMJ, Article 134**

In Specification 12 of Charge II, the accused is charged with stealing or converting the Department of State Net-Centric Diplomacy database containing more than 250,000 records belonging to the United States government, of a value of more than \$1,000, in violation of 18 U.S.C. § 641. To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 4 May 2010, the accused did knowingly and willfully steal, purloin, or convert to his use or the use of another a record or thing of value, to wit: the Department of State Net-Centric Diplomacy database containing more than 250,000 records;

(2) That the Net-Centric Diplomacy database belonged to the United States government or a department or agency thereof;

(3) That the Net-Centric Diplomacy database was of a value of more than \$1,000;

(4) That the taking by the accused was with the intent to deprive the United States government of the use or benefit of the property;

(5) That, at the time, 18 U.S.C. § 641 was in existence; and

(6) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchbook*, paragraph 2-5-9; 18 U.S.C. § 641; Model Crim. Jury Instr. 8th Cir. 6.18.641 (2011) (Enclosure 3).

Lesser-Included Offense

The offense of stealing or converting the Net-Centric Diplomacy database, of a value of less than \$1,000, is a lesser-included offense of the offense set forth in Specification 12 of Charge II. When you vote, if you find the accused not guilty of the offense charged, that is, stealing or converting the Net-Centric Diplomacy database, of a value of more than \$1,000, then you should consider the lesser-included offense of stealing or converting the Net-Centric Diplomacy database, of a value of less than \$1,000, in violation of 18 U.S.C. § 641. To find the accused guilty of this lesser offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of all of the elements of the greater offense, except for the value element. The offense charged, and the lesser-included offense of stealing or converting the Net-Centric Diplomacy database, of a value of less than \$1,000, differ in that the greater offense requires you to be satisfied beyond a reasonable doubt that the Net-Centric Diplomacy database is worth more than \$1,000.

Adapted from *Benchbook*, paragraph 2-5-10.

**Specification 13 of Charge II: Violation of the UCMJ, Article 134<sup>8</sup>**

In Specification 13 of Charge II, the accused is charged with exceeding authorized access on a computer and obtaining classified Department of State cables, in violation of 18 U.S.C. § 1030(a)(1). To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010, the accused knowingly exceeded authorized access on a Secret Internet Protocol Router Network computer;

(2) That the accused, by that means, obtained information that has been determined by the United States government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, to wit: more than seventy-five classified Department of State cables;

(3) That the accused willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, the more than seventy-five Department of State cables, to a person not entitled to receive them;

(4) That the accused had reason to believe that the Department of State cables could be used to the injury of the United States or to the advantage of any foreign nation;

---

<sup>8</sup> The United States requests that Proposed Instructions 1-10 be given for Specification 14 as well.

(5) That, at the time, 18 U.S.C. § 1030(a)(1) was in existence; and

(6) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchbook*, paragraph 2-5-9; 18 U.S.C. § 1030(a)(1); Model Crim. Jury Instr. 9th Cir. 8.95 (2010) (Enclosure 5).

#### Lesser-Included Offense

The offense of conduct prejudicial to good order and discipline and service discrediting is a lesser-included offense of the offense set forth in Specification 13 of Charge II. When you vote, if you find the accused not guilty of the offense charged, that is, exceeding authorized access on a SIPRNET computer in violation of 18 U.S.C. § 1030(a)(1), then you should next consider the lesser-included offense of conduct prejudicial to good order and discipline and service discrediting, in violation of Article 134. To find the accused guilty of this lesser offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010, the accused [x]; and

(2) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

The offense charged, exceeding authorized access on a SIPRNET computer in violation of 18 U.S.C. § 1030(a)(1), and the lesser-included offense of a violation of Article 134, differ primarily in that the offense charged requires as [an] essential element[s] that you be convinced beyond a reasonable doubt that [elements], whereas the lesser offense of a violation of Article 134 does not include such [an] element[s], but it does require that you be satisfied beyond a reasonable doubt that [the accused committed an act] and that, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchbook*, paragraph 2-5-10.

#### Proposed Instruction No. 1

Title 18, United States Code, Section 1030(a)(1) makes it a crime to knowingly access a computer in excess of authorization for the purpose of obtaining classified information. Although there is considerable overlap between 18 U.S.C. Section 1030(a)(1) and 18 U.S.C. 793(e), Section 1030(a)(1) is focused on the individual's use of a computer.

S. Rep. No. 104-357, at 6 (1996).

Proposed Instruction No. 2

The term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.

18 U.S.C. § 1030(e)(1).

Proposed Instruction No. 3

The term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter. "Exceeds authorized access" under § 1030(a)(1) is limited to violations of restrictions on access to information, and not restrictions on its use. In deciding whether the accused "exceeded authorized access" to the State Department cables at issue, you may consider all the evidence introduced at trial, including any evidence concerning the use of unauthorized software to obtain the cables and any access limitations or restrictions to the State Department cables, or lack thereof, on the SIPRNET. The words "access" and "use" are commonly used and commonly understood words.

18 U.S.C. § 1030(e)(6); *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012).

Proposed Instruction No. 4<sup>9</sup>

"Reason to believe" means that the accused knew facts from which he concluded or reasonably should have concluded that the information could be used for the prohibited purposes. In considering whether the accused had reason to believe that the information could be used to the injury of the United States or to the advantage of a foreign country, you may consider the nature of the information involved. You need not determine that the accused had reason to believe that the information would be used against the United States, only that it could be so used.

*United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Diaz*, 69 M.J. 127 (C.A.A.F. 2010) (Enclosure 2 at 5); *United States v. Regan* (Enclosure 7 at 17-18); *see also* Mod. Fed. Jury Instr. (Enclosure 6) (citing *Truong*).

Proposed Instruction No. 5

The government does not have to prove that the accused had reason to believe that his act could both injure the United States and be to the advantage of a foreign country – the statute reads in

---

<sup>9</sup> Proposed Instructions 4 and 5 mirror the instructions given under 18 U.S.C. § 793(e). As the Senate Report to the 1996 amendments noted, § 1030(a)(1) was amended to track the scienter requirement of § 793(e). S. Rep. No. 104-357, at 6 (1996).

the alternative. Also, the country to whose advantage the information could be used need not necessarily be an enemy of the United States. The statute does not distinguish between friend and enemy.

*United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Diaz*, 69 M.J. 127 (C.A.A.F. 2010) (Enclosure 2 at 5-6); *United States v. Regan* (Enclosure 7 at 17-18); *see also* Mod. Fed. Jury Instr. (Enclosure 6) (citing *Truong*).

#### Proposed Instruction No. 6

An act is done “knowingly” if it is done voluntarily and intentionally and not because of mistake or accident or other innocent reason.

*United States v. Fowler*, 932 F.2d 306 (4th Cir. 1991); *United States v. McGahee*, 257 F.3d 520 (6th Cir. 2001); *see also* Enclosure 5 (referencing 9th Circuit Instruction 5.6 defining “knowingly”).

#### Proposed Instruction No. 7

An act is done “willfully” if it is done voluntarily and intentionally and with the specific intent to do something that the law forbids; that is, with a bad purpose either to disobey or to disregard the law.

*United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988) (Enclosure 1 at 199); *United States v. Diaz*, 69 M.J. 127 (C.A.A.F. 2010) (Enclosure 2 at 6); *see also* Mod. Fed. Jury Instr. (Enclosure 6).

#### Proposed Instruction No. 8<sup>10</sup>

In determining whether the person who received the information was entitled to have it, you may consider all the evidence introduced at trial, including any evidence concerning the classification status of the information, any evidence relating to law and regulations governing the classification and declassification of national security information, its handling, use, and distribution, as well as any evidence relating to regulations governing the handling, use, and distribution of information obtained from classified systems.

Adapted from *United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988); *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Diaz*, 69 M.J. 127 (C.A.A.F. 2010) (Enclosure 2 at 6); *see also* Mod. Fed. Jury Instr. (Enclosure 6).

#### Proposed Instruction No. 9

The term “person” means any individual, firm, corporation, education institution, financial institution, governmental entity, or legal or other entity.

---

<sup>10</sup> This instruction tracks the “entitled to receive” instruction given for § 793(e) offenses.

18 U.S.C. § 1030(e)(12).

Proposed Instruction No. 10

I have taken judicial notice that Title 18, United States Code Section 1030(a)(1) was in existence on the date alleged in the specification

**Specification 14 of Charge II: Violation of the UCMJ, Article 134**

In Specification 14 of Charge II, the accused is charged with exceeding authorized access on a computer and obtaining a classified Department of State cable titled "Reykjavik-13", in violation of 18 U.S.C. § 1030(a)(1). To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 15 February 2010 and on or about 18 February 2010, the accused knowingly exceeded authorized access on a Secret Internet Protocol Router Network computer;

(2) That the accused, by that means, obtained information that has been determined by the United States government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, to wit: a classified Department of State cable titled "Reykjavik-13";

(3) That the accused willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, "Reykjavik-13", to a person not entitled to receive it;

(4) That the accused had reason to believe that "Reykjavik-13" could be used to the injury of the United States or to the advantage of any foreign nation;

(5) That, at the time, 18 U.S.C. § 1030(a)(1) was in existence; and

(6) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchmark*, paragraph 2-5-9; 18 U.S.C. § 1030(a)(1); Model Crim. Jury Instr. 9th Cir. 8.95 (2010) (Enclosure 5).

Lesser-Included Offense

The offense of conduct prejudicial to good order and discipline and service discrediting is a lesser-included offense of the offense set forth in Specification 14 of Charge II. When you vote, if you find the accused not guilty of the offense charged, that is, exceeding authorized access on a SIPRNET computer in violation of 18 U.S.C. § 1030(a)(1), then you should next consider the lesser-included offense of conduct prejudicial to good order and discipline and service discrediting, in violation of Article 134. To find the accused guilty of this lesser offense, you

must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 15 February 2010 and on or about 18 February 2010, the accused [x]; and

(2) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

The offense charged, exceeding authorized access on a SIPRNET computer in violation of 18 U.S.C. § 1030(a)(1), and the lesser-included offense of a violation of Article 134, differ primarily in that the offense charged requires as [an] essential element[s] that you be convinced beyond a reasonable doubt that [elements], whereas the lesser offense of a violation of Article 134 does not include such [an] element[s], but it does require that you be satisfied beyond a reasonable doubt that [the accused committed an act] and that, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchmark*, paragraph 2-5-10.

#### **Specification 15 of Charge II: Violation of the UCMJ, Article 134**

In Specification 15 of Charge II, the accused is charged with transmitting a classified record from a United States Army intelligence organization to a person not entitled to receive it, in violation of 18 U.S.C. § 793(e). To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 15 February 2010 and on or about 15 March 2010, the accused had possession of information relating to the national defense, to wit: a classified record from a United States Army intelligence organization, dated 18 March 2008;

(2) That the possession was unauthorized;

(3) That the accused had reason to believe that such information could be used to the injury of the United States or to the advantage of any foreign nation;

(4) That the accused willfully communicated, delivered, transmitted, or caused to be communicated, delivered, or transmitted, the said information, to a person not entitled to receive it;

(5) That, at the time, 18 U.S.C. § 793(e) was in existence; and



(6) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchbook*, paragraph 2-5-9; 18 U.S.C. § 793(e).

#### **Specification 16 of Charge II: Violation of the UCMJ, Article 134**

In Specification 16 of Charge II, the accused is charged with stealing or converting the United States Forces – Iraq Microsoft Outlook / SharePoint Exchange Server global address list, of a value of more than \$1,000, in violation of 18 U.S.C. § 641. To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 11 May 2010 and on or about 27 May 2010, the accused did knowingly and willfully steal, purloin, or convert to his use or the use of another a record or thing of value, to wit: the United States Forces – Iraq Microsoft Outlook / SharePoint Exchange Server global address list;

(2) That the USF-I GAL belonged to the United States government or a department or agency thereof;

(3) That the USF-I GAL was of a value of more than \$1,000;

(4) That the taking by the accused was with the intent to deprive the United States government of the use or benefit of the property;

(5) That, at the time, 18 U.S.C. § 641 was in existence; and

(6) That, under the circumstances, the conduct of the accused (was to the prejudice of good order and discipline in the armed forces) (and) (was of a nature to bring discredit upon the armed forces).

Adapted from *Benchbook*, paragraph 2-5-9; 18 U.S.C. § 641; Model Crim. Jury Instr. 8th Cir. 6.18.641 (2011) (Enclosure 3).

#### **Lesser-Included Offense**

The offense of stealing or converting the USF-I GAL, of a value of less than \$1,000, is a lesser-included offense of the offense set forth in Specification 16 of Charge II. When you vote, if you find the accused not guilty of the offense charged, that is, stealing or converting the USF-I GAL, of a value of more than \$1,000, then you should consider the lesser-included offense of stealing or converting the USF-I GAL, of a value of less than \$1,000, in violation of 18 U.S.C. § 641. To find the accused guilty of this lesser offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of all of the elements of the greater offense, except for the

value element. The offense charged, and the lesser-included offense of stealing or converting the USF-I GAL, of a value of less than \$1,000, differ in that the greater offense requires you to be satisfied beyond a reasonable doubt that the USF-I GAL is worth more than \$1,000.

Adapted from *Benchbook*, paragraph 2-5-10.

### **Specification 1 of Charge III: Violation of the UCMJ, Article 92**

In Specification 1 of Charge III, the accused is charged with violating paragraph 4-5(a)(4) of Army Regulation 25-2. To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That there was in existence a certain lawful general regulation in the following terms: paragraph 4-5(a)(4), Army Regulation 25-2, dated 24 October 2007;

(2) That the accused had a duty to obey such regulation; and

(3) That at or near Contingency Operating Station Hammer, Iraq, between on or about 1 November 2009 and on or about 8 March 2010, the accused violated this regulation by attempting to bypass network or information system security mechanisms.

Adapted from *Benchbook*, paragraph 3-16-1.

#### Proposed Instruction No. 1<sup>11</sup>

I have taken judicial notice that Army Regulation 25-2 is a lawful general regulation.

Adapted from *Benchbook*, paragraph 3-16-1.

#### Proposed Instruction No. 2

General regulations are those regulations which are generally applicable to an armed force and which are properly published by the President, the Secretary of Defense, or Department of the Army.

Adapted from *Benchbook*, paragraph 3-16-1.

#### Proposed Instruction No. 3

AR 25-2 defines an "information system" as a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system applications, enclaves, outsourced information technology-based processes, and platform information technology interconnections.

---

<sup>11</sup> This instruction for Specifications 1-5 of Charge III assumes the Court takes judicial notice of Army Regulations 25-2 and 380-5.

Army Regulation 25-2, dated 24 October 2007, at 86.

Proposed Instruction No. 4

AR 25-2 defines a “network” as a communications medium and all components attached to that medium whose function is the transfer of information. Components may include information systems, packet switches, telecommunications controllers, key distribution centers, and technical control devices.

Army Regulation 25-2, dated 24 October 2007, at 89.

**Specification 2 of Charge III: Violation of the UCMJ, Article 92**

In Specification 2 of Charge III, the accused is charged with violating paragraph 4-5(a)(3) of Army Regulation 25-2. To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That there was in existence a certain lawful general regulation in the following terms: paragraph 4-5(a)(3), Army Regulation 25-2, dated 24 October 2007;

(2) That the accused had a duty to obey such regulation; and

(3) That at or near Contingency Operating Station Hammer, Iraq, between on or about 11 February 2010 and on or about 3 April 2010, the accused violated this regulation by adding unauthorized software to a Secret Internet Protocol Router Network computer.

Adapted from *Benchbook*, paragraph 3-16-1.

Proposed Instruction No. 1

I have taken judicial notice that Army Regulation 25-2 is a lawful general regulation.

Adapted from *Benchbook*, paragraph 3-16-1.

Proposed Instruction No. 2

General regulations are those regulations which are generally applicable to an armed force and which are properly published by the President, the Secretary of Defense, or Department of the Army.

Adapted from *Benchbook*, paragraph 3-16-1.

Proposed Instruction No. 3

“Software” is a collection of computer programs and related data that provides the instructions for telling a computer what to do and how to do it.

Proposed Instruction No. 4

“Unauthorized software” under AR 25-2 includes, but is not limited to, commercial instant messaging, commercial Internet chat, collaborative environments, or peer-to-peer client applications, or applications that create exploitable vulnerabilities and circumvent normal means of securing and monitoring network activity and provide a vector for the introduction of malicious code, remote access, network intrusions, or the exfiltration of protected data.

Army Regulation 25-2, paragraph 4-5(a)(3).

Proposed Instruction No. 5

In determining whether “Wget” was unauthorized software, you may consider all the evidence introduced at trial.

**Specification 3 of Charge III: Violation of the UCMJ, Article 92**

In Specification 3 of Charge III, the accused is charged with violating paragraph 4-5(a)(3) of Army Regulation 25-2. To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That there was in existence a certain lawful general regulation in the following terms: paragraph 4-5(a)(3), Army Regulation 25-2, dated 24 October 2007;

(2) That the accused had a duty to obey such regulation; and

(3) That at or near Contingency Operating Station Hammer, Iraq, on or about 4 May 2010, the accused violated this regulation by adding unauthorized software to a Secret Internet Protocol Router Network computer.

Adapted from *Benchbook*, paragraph 3-16-1.

Proposed Instruction No. 1

I have taken judicial notice that Army Regulation 25-2 is a lawful general regulation.

Adapted from *Benchbook*, paragraph 3-16-1.

Proposed Instruction No. 2

General regulations are those regulations which are generally applicable to an armed force and which are properly published by the President, the Secretary of Defense, or Department of the Army.

Adapted from *Benchbook*, paragraph 3-16-1.

Proposed Instruction No. 3

“Software” is a collection of computer programs and related data that provides the instructions for telling a computer what to do and how to do it.

Proposed Instruction No. 4

“Unauthorized software” under AR 25-2 includes, but is not limited to, commercial instant messaging, commercial Internet chat, collaborative environments, or peer-to-peer client applications.

Army Regulation 25-2, paragraph 4-5(a)(3).

Proposed Instruction No. 5

In determining whether “Wget” was unauthorized software, you may consider all the evidence introduced at trial.

**Specification 4 of Charge III: Violation of the UCMJ, Article 92**

In Specification 4 of Charge III, the accused is charged with violating paragraph 4-5(a)(3) of Army Regulation 25-2. To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

- (1) That there was in existence a certain lawful general regulation in the following terms: paragraph 4-5(a)(3), Army Regulation 25-2, dated 24 October 2007;
- (2) That the accused had a duty to obey such regulation; and
- (3) That at or near Contingency Operating Station Hammer, Iraq, between on or about 11 May 2010 and on or about 27 May 2010, the accused violated this regulation by using an information system in a manner other than its intended purpose.

Adapted from *Benchbook*, paragraph 3-16-1.

Proposed Instruction No. 1

I have taken judicial notice that Army Regulation 25-2 is a lawful general regulation.

Adapted from *Benchbook*, paragraph 3-16-1.

### Proposed Instruction No. 2

General regulations are those regulations which are generally applicable to an armed force and which are properly published by the President, the Secretary of Defense, or Department of the Army.

Adapted from *Benchbook*, paragraph 3-16-1.

### Proposed Instruction No. 3

AR 25-2 defines an “information system” as a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system applications, enclaves, outsourced information technology-based processes, and platform information technology interconnections.

Army Regulation 25-2, dated 24 October 2007, at 86.

### **Specification 5 of Charge III: Violation of the UCMJ, Article 92**

In Specification 5 of Charge III, the accused is charged with violating paragraph 7-6 of Army Regulation 380-5. To find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond a reasonable doubt of the following elements:

(1) That there was in existence a certain lawful general regulation in the following terms: paragraph 7-6, Army Regulation 380-5, dated 29 September 2000;

(2) That the accused had a duty to obey such regulation; and

(3) That at or near Contingency Operating Station Hammer, Iraq, between on or about 1 November 2009 and on or about 27 May 2010, the accused violated this regulation by wrongfully storing classified information.

Adapted from *Benchbook*, paragraph 3-16-1.

### Proposed Instruction No. 1

I have taken judicial notice that Army Regulation 380-5 is a lawful general regulation.

Adapted from *Benchbook*, paragraph 3-16-1.

### Proposed Instruction No. 2

General regulations are those regulations which are generally applicable to an armed force and which are properly published by the President, the Secretary of Defense, or Department of the Army.

Adapted from *Benchbook*, paragraph 3-16-1.

Proposed Instruction No. 3

“Wrongfully” means without legal justification or excuse.

*Benchbook*, paragraph 3-60-2A, NOTE 3.


Proposed Instruction No. 4

“Classified information” means information and material that has been determined, pursuant to Executive Order 13526 or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary or readable form.

Adapted from Army Regulation 380-5, dated 29 September 2000, at 227.

CONCLUSION


The United States respectfully requests this Court adopt the Government’s proposed member instructions for the charged offenses and lesser-included offenses listed above.

  
JODEAN MORROW  
CPT, JA  
Trial Counsel

7 Encls

1. Transcript, *Morison*
2. Transcript, *Diaz*
3. 8th Cir. Instr. § 641
4. 5th Cir. Instr. § 641
5. 9th Cir. Instr. § 1030(a)(1)
6. Mod. Fed. Jury Instr. § 793(e)
7. Transcript, *Regan*

I certify that I served or caused to be served a true copy of the above on Mr. David E. Coombs, Civilian Defense Counsel, via electronic mail, on 22 June 2012.

  
JODEAN MORROW  
CPT, JA  
Trial Counsel



UNITED STATES OF AMERICA

v.

Manning, Bradley E.

PFC, U.S. Army,

HHC, U.S. Army Garrison,

Joint Base Myer-Henderson Hall

Fort Myer, Virginia 22211

GOVERNMENT PROPOSED  
MEMBER INSTRUCTIONS

Enclosure 1

21 June 2012

1 that Process I urge you to return to this room and tell the  
2 defendant that he is guilty on all 4 counts. Thank You.

3 THE COURT: Members of the jury, I am going to be  
4 about half an hour. Does anybody want to take a brief  
5 recess before I begin? You do? Anybody want to take a brief  
6 recess? Okay. Just about 5 minutes. Hurry back please.  
7 Don't discuss the case.

8 JURY NOT PRESENT

9 RECESS

10 JURY PRESENT

11 THE COURT: Members of the jury, first let me, as  
12 counsel have already done, thank you for your attention that  
13 you have given to counsel and the witnesses who have  
14 testified during the trial of this case, also to thank you  
15 for your understanding and patience when we have had certain  
16 delays that have occurred during the course of the  
17 proceedings. I thank you for all of this.

18 As you may already know, the functions of a judge and a  
19 jury in a case such as this are quite different. It is my  
20 duty as judge to instruct you on the law that applies to the  
21 case. It is your duty as jurors to decide the facts of the  
22 case. In doing so you must apply the law as I state it to you  
23 without regard to what you think the law is or what you think  
24 it should be. In deciding the facts and the issues of fact  
25 you must decide them without prejudice or bias or sympathy.

1 You should not single out any certain individual sentence and  
2 ignore the others. Rather, you should consider all of the  
3 instructions as a whole and regard each instruction in the  
4 light of all the others. As jurors, you and only you are the  
5 judges of the facts of this case. If any expression of mine,  
6 or anything I may or may not have done or said would seem to  
7 indicate any opinion that relates to a factual matter I  
8 instruct you to disregard it. In the course of instructing  
9 you on the law of this case I may refer to some of the  
10 evidence in the case. In their arguments counsel also  
11 referred, of course, to the evidence in the case. You are by  
12 no means restricted to the evidence to which I may refer or  
13 to which counsel may have referred. In determining the guilt  
14 or innocence of the defendant you may consider any testimony  
15 or any exhibit that has been produced during the course of  
16 the trial. You are to consider only the evidence that has  
17 been presented during the trial, but you are not limited to  
18 the bald statements of the witnesses or the literal meaning  
19 of the exhibits that you have in evidence. You are permitted  
20 to draw any reasonable inference that would be suggested by  
21 the facts as you find those facts. You have heard counsel  
22 outline their cases at the beginning of the trial; and they  
23 asked questions of witnesses during the course of the trial;  
24 and you have heard their closing arguments to you. As I  
25 indicated to you before, and I remind you again, the

statements in the arguments of counsel are not evidence in the case. The only exception to this relates to stipulations, if there are any that have been agreed upon. In this case there is one stipulation agreed to by counsel for the Government and the defendant; and you may accept that stipulation as evidence and regard that fact as conclusively determined. And that stipulation was made for the purpose of this case and indicates and agrees that the KH-11, the satellite about which you have heard testimony, was operating in 1984 as it has been indicated and depicted in the manual that had been issued in 1976.

During the course of the trial I have been called upon to make rulings on admissibility of certain offered evidence. You should not be concerned with my rulings or the reasons for those rulings because the admissibility of evidence is purely a question of law. When I admitted evidence despite counsel's objections you should not infer that that evidence is any more or less valuable than any other evidence. If I sustained an objection and did not allow a witness to answer a question you must not guess what the answer might have been. You must not speculate as to the reason the question was asked or the reason for the objection. The defendant has the right to object to any evidence offered against him and to obtain the legal opinion of the Court as to whether that evidence is admissible, and if admissible for what purposes.

1 and to what extent. You are not to infer that any objections  
2 to evidence had any other Purpose. The same, of course, is  
3 true with respect to objections which may have been made by  
4 the Government. Any evidence to which an objection was  
5 sustained by the Court and evidence that was ordered stricken  
6 by the Court must be entirely disregarded by you.

7 As you know, this is a criminal case; and there are  
8 certain rules, general rules, that apply to criminal cases as  
9 such. First let me refer to the indictment. You will have a  
10 copy of that to take into the jury room. That is simply a  
11 formal method of accusing the defendant of a crime. It is  
12 not evidence against the accused; and it does not create any  
13 presumption that the defendant is guilty. And by filing  
14 Pleas of not guilty to each of the 4 counts of the indictment  
15 the defendant has challenged the Government to prove in Court  
16 every fact that is alleged in the indictment. Further, the  
17 Pleas of not guilty serve as a continuing denial by the  
18 defendant of all the evidence offered against him by the  
19 prosecution.

20 Another rule that applies to criminal cases is that a  
21 defendant is presumed to be innocent. The defendant, even  
22 though accused of a crime, begins the trial with a clean  
23 slate, and that is to say with no evidence against him. The  
24 Government has the burden of proving that the defendant is  
25 guilty beyond a reasonable doubt. From the beginning of the

1 trial, then, to the end of the trial the Government has the  
2 burden of establishing beyond a reasonable doubt every fact  
3 that is essential to the conviction of the defendant. The  
4 defendant has no burden of Proof and no duty to Prove he did  
5 not commit the alleged crime. The Government is required to  
6 Prove, as I have indicated, that the defendant is Guilty  
7 beyond a reasonable doubt; and that means that to convict the  
8 defendant You must not have a reasonable doubt as to his  
9 Guilt. You must be convinced to a moral certainty that the  
10 defendant is Guilty. If You are not convinced to a moral  
11 certainty, if You have a reasonable doubt, then You must find  
12 the defendant not Guilty to that count or as to those counts  
13 as to which You have that Particular feeling. A reasonable  
14 doubt may arise not only from the evidence Produced but also  
15 from a lack of evidence. As I have indicated, the Government  
16 has the burden to Prove the defendant Guilty beyond a  
17 reasonable doubt of every essential element of the Crimes as  
18 charged; and the defendant has no burden to Put on any  
19 evidence. In determining whether the Government has Proven  
20 its case You also may consider testimony that counsel for the  
21 defendant has brought out in cross examining witnesses who  
22 were called by the Government to testify.

23 There are two types of evidence from which You, as  
24 Jurors, may Properly find a defendant Guilty of an offense.  
25 One is direct evidence, such as the testimony of, for

1 example, a witness who is reporting on something that he or  
2 she has observed and is reporting on that. The other is  
3 circumstantial evidence. That is, the proof of a chain of  
4 circumstances that suggests that a defendant committed an  
5 offense. As a general rule the law makes no distinction  
6 between direct and circumstantial evidence, simply requiring  
7 that before convicting a defendant you must be convinced of  
8 the defendant's guilt beyond a reasonable doubt from all the  
9 evidence in the case.

10 As jurors, you are the sole judge of the credibility of  
11 the witnesses and the weight that their testimony deserves.  
12 You should carefully scrutinize the testimony given by each  
13 witness who has testified, the circumstances under which the  
14 witness has testified and every matter that is in evidence  
15 that indicates to you whether or not a witness is worthy of  
16 belief. You should consider the witness's intelligence, the  
17 motive, the state of mind, the demeanor and the manner of the  
18 witness while on the stand testifying. You should also  
19 consider any relation that a witness may bear to either side  
20 of the case, the manner in which the witness might be  
21 affected by the verdict and the extent to which, if at all,  
22 the testimony of a witness is either supported or  
23 contradicted by other evidence. Inconsistency or a  
24 discrepancy in the testimony of witnesses may or may not  
25 cause you to discredit parts of that testimony. 2 or more

1 individuals who are reporting on a Particular matter may  
2 report it differently; and it is not uncommon for People to  
3 forget something or to remember it incorrectly. You should,  
4 therefore, consider any inconsistencies or discrepancies in  
5 testimony as well as any vagueness or limited recollection on  
6 the part of witnesses. But, in weighing the effect, consider  
7 whether or not the inconsistency or the vagueness Pertains to  
8 some important Part or to some unimportant detail and whether  
9 or not the inconsistency or the vagueness results from some  
10 innocent mistake or from a deliberate falsehood.

11 During the trial you have heard and seen two video taped  
12 depositions that have been Presented to you. Those consist  
13 of sworn answers to questions that were asked by attorneys in  
14 the case at a Prior time. Those two witnesses were Derek  
15 Wood and Sydney Jackson, the editor-in-chief and the managing  
16 editor, respectively, of Jane's Weekly, a British Publication.  
17 That video taped testimony is entitled to the same  
18 consideration as any testimony given in the courtroom. And  
19 that is that you should judge it as to credibility. You  
20 should weigh it and otherwise consider it in the same way as  
21 if the witness had been Present and had testified during the  
22 course of the trial. Also, as to those two witnesses, Mr.  
23 Wood and Mr. Jackson, you recall that there was reference to  
24 immunity that had been Granted to them Prior to them giving  
25 testimony relating to this case. An individual who testifies



1 under a grant of immunity with a promise from the government  
2 that he will not be prosecuted is none the less a competent  
3 witness. That testimony should be examined by you, however,  
4 with greater care than the testimony of an ordinary witness;  
5 and you should consider whether or not the testimony may be  
6 colored in such a way as to further that witness's own  
7 interests. After the consideration that you give to that  
8 testimony, you may give the testimony of the immunized  
9 witness such weight as you may feel it deserves.

10 Now, the rules of evidence permit certain individuals to  
11 testify as to opinions or conclusions. Individuals who  
12 testify as such are referred to as expert witnesses. These  
13 are individuals who, because of education or experience have  
14 become expert in some art or some particular profession or  
15 science; and they may state an opinion as to relevant and  
16 material matters in which they profess to be experts. They  
17 may also state their reasons for that opinion. You should  
18 consider those expert opinions that have been received in  
19 evidence in this case; and you should give them such weight  
20 as you may think they deserve. The weight that is to be  
21 given an expert opinion may depend upon the education, the  
22 position and the experience of the witness and the reasons  
23 that are given in support of the opinion and the strength or  
24 any other evidence that bear upon the same issue. You recall  
25 that during the course of the trial a number of individuals

1 were qualified to testify as experts. On behalf of the  
2 Government You heard the testimony of Richard Hineman, who  
3 is with the CIA, of Robert Chapin with the Navy, of Rutledge  
4 Hazzard, a General with the Army, and of Richard Kerr with  
5 the CIA. You also heard the testimony of, on behalf of the  
6 defendant, of Jeffrey Richelson, of John Pike and Roland  
7 Inlow. I think it is fair to state that there are  
8 differences in some of the opinions that these witnesses  
9 gave. They testified relating to whether or not there was  
10 potential damage and whether or not the issues related to  
11 this case had been subject to Public disclosure. As I say,  
12 you are to consider what you heard from those witnesses; and  
13 if you find a conflict in their opinions then you may resolve  
14 that conflict by considering their respective educations,  
15 positions and the experience of the witnesses as well as  
16 whether or not the reasons that they gave in support of their  
17 opinions justify those opinions as well as all of the other  
18 evidence in the case. After you have considered all of the  
19 factors that I have referred to that bear upon the  
20 credibility of a witness you may decide to reject some or all  
21 or none of the testimony of any particular witness. In other  
22 words, give the testimony of any witness whatever weight you,  
23 as jurors, may think it deserves.

24 The law does not require a defendant to take the stand and  
25 testify; and the defendant chose not to do so. That was his

1 right. You may not infer from his decision not to testify  
2 that he is more likely to be guilty than if he had chosen to  
3 testify.

4 Now, I have referred to the indictment, simply  
5 indicating that you would have a copy of it and as to what  
6 effect it has in this case. You will have that, as I say, to  
7 take with you into the jury room. You will note there are a  
8 number of counts. Specifically there are 4 counts in the  
9 indictment. Each count represents a separate criminal charge  
10 against the defendant; and I will explain to you now what you  
11 need to know to reach a verdict as to each of those counts;  
12 and under each of the counts I will refer to what are so  
13 called essential elements of the crime that is charged in  
14 those counts. The government must prove all of those  
15 elements of a crime to prove that the defendant is guilty of  
16 that crime. If you have a reasonable doubt as to one or more  
17 of the essential elements of a crime then you must find the  
18 defendant not guilty of that crime.

19 Now, the first count, count 1 of the indictment is  
20 brought under a particular provision of the United States  
21 Code, specifically Title 18, the section that is known as 93,  
22 a portion of that. Let me refer to it just briefly and to  
23 quote it to you, at least the relevant portions. It reads:

24 "Whoever lawfully having access to any photograph  
25 relating to the national defense willfully

1 communicates, delivers, transmits or causes to be  
2 communicated, delivered or transmitted the same to  
3 any Person not entitled to receive it shall be  
4 guilty of an offense against the laws of the United  
5 States."

6 Now, you will recall, as counsel have argued to you and  
7 from the evidence in the case, that count 1 refers to the  
8 photographs that were published in Jane's Defense Weekly and  
9 also the Naval report that was published relating to those  
10 photographs. There are 3 essential elements that must be  
11 proved to establish the offense that is charged in the first  
12 count. And that is, first, that the defendant, Samuel  
13 Morison, had lawful access to the photographs that are  
14 referred to in count 1. Secondly, that on or about the date  
15 that is alleged in the first count of the indictment the  
16 defendant, Samuel Morison willfully caused the photographs to  
17 be delivered and transmitted to a Person who was not entitled  
18 to receive them. And third, that the photographs that were  
19 delivered and transmitted related to the national defense.

20 Now, the third count of the indictment is also brought  
21 under a Particular Portion of the United States Code, another  
22 portion of section 793. And a Particular Part of that reads  
23 as follows:

24 "Whoever having unauthorized possession of any  
25 document or writing relating to the national defense

1 willfully retains the same and fails to deliver it to  
2 the officer or employee of the United States entitled  
3 to receive it shall be guilty of an offense against  
4 the laws of the United States."

5 Again, count 3 refers to the documents that have been  
6 referred to as excerpts from the weekly wires relating to the  
7 explosion at Severomorsk that were found, according to the  
8 testimony, in the defendant's home. There are 3 essential  
9 elements to be proven to establish the offense as charged in  
10 the third count of the indictment. ✓ First, that the  
11 defendant, Samuel Morison, had unauthorized possession of  
12 portions of the documents and writings that are referred to  
13 in that count, count 3. ✓ Secondly, that on or about the dates  
14 that are referred to in count 3 of the indictment the  
15 defendant did willfully retain those documents and the  
16 writings that were referred to in that count and failed to  
17 deliver them to the officer or employee of the United States  
18 who was entitled to receive them. ✓ And third, that the  
19 documents that were willfully retained and not delivered were  
20 documents relating to the national defense. ✓ An individual  
21 has unauthorized possession of documents and writings when he  
22 possesses those under circumstances or in a location which is  
23 contrary to law or regulation for the conditions of his  
24 employment.

25 Now, I referred to both counts so far, 1 and 3; and

1 there are certain matters I've referred to that must be  
2 proven in that. Let me just say a few more words about  
3 those. As to both counts, counts 1 and 3, the Government  
4 must prove that the specific items, either the photographs as  
5 they relate to count 1 or the documents as they relate to  
6 count 3, relate to the national defense. You will recall  
7 that was the wording that was used in both of the relevant  
8 sections of the United States Code. And this is a question  
9 of facts solely for determination by you as jurors. It is  
10 not necessary for the Government that all parts of the  
11 documents or the photographs relate to national defense. To  
12 establish this element of the defense the Government has to  
13 prove that some part of the documents and/or the photographs  
14 are related to national defense. And that term, the term  
15 national defense, includes all matters that directly or may  
16 reasonably be connected with the defense of the United States  
17 against any of its enemies. It refers to the military and  
18 naval establishments and the related activities of national  
19 preparedness. To prove that the documents or the photographs  
20 relate to national defense there are two things that the  
21 Government must prove. First, it must prove that the  
22 disclosure of the photographs would be potentially damaging  
23 to the United States or might be useful to an enemy of the  
24 United States. Secondly, the Government must prove that the  
25 documents or the photographs are closely held, in that the

1 relevant Government agency has sought to keep the information  
2 from the public generally, and the documents or photographs  
3 have not been made public and are not available to the  
4 general public. Evidence that a document or photograph was  
5 at the time of the offense that is charged marked, classified  
6 as secret may be some evidence that the document or  
7 photographs and its contents relate to the national defense.  
8 You are free to give such classification any weight that any  
9 of you may think it is entitled to have. You may totally  
10 disregard the fact of classification if you conclude that  
11 that fact is not entitled to any weight in this case.  
12 Whether or not a document or photograph is classified secret  
13 is not conclusive as to whether it does or does not relate to  
14 the national defense. The Government is not required to  
15 prove that the document or the photographs were in fact  
16 properly classified as secret. It is for you as members of  
17 the jury to determine from all the evidence whether the  
18 documents or the photographs referred to in the indictment  
19 relate to the national defense.

20 Now, I have referred to counts 1 and 3 relating to the  
21 charges as they relate to the photographs and the documents,  
22 the weekly wires. Counts 2 and 4 are similar in that they  
23 are both brought under the same Title of the United States  
24 Code, Title 18, but they are brought under a different  
25 section -- but both are brought under the same section.

different, however, than 1 and 3. That is Section 641. The statute that relates to that under 641 states in Part:

"Whoever embezzles, steals or knowingly converts to his own use or the use of another or without authority sells or conveys or disposes of anything of value of the United States or of any department or agency thereof which has a value in excess of the sum of \$100 shall be guilty of an offense against the laws of the United States."

Again, there are certain essential elements the Government must prove beyond a reasonable doubt to establish the offense that is described in counts 2 and 4. First, that the thing of value as described in the indictment under 2 and 4 belong to the United States or an agency or department thereof, and have a value in excess of \$100. Secondly, that the defendant embezzled or stole or purloined or converted those things of value to his own use or to the use of another or that he did that without authority, knowingly and willfully, and did sell and convey, dispose of those things of value knowingly and willfully. Third, that the defendant knowingly and willfully and without authority with intent to deprive the owner of the use of the benefit of the thing of value so taken, that he did those acts knowingly and willfully, as I have indicated.

Now, the statute uses the words to steal and convert;



1 and those words simply mean wrongful or willful taking of  
2 something that belongs to another with the intent to deprive  
3 the owner of its use or benefit either temporarily or  
4 permanently. No particular type of movement or carrying away  
5 is required to constitute what is stated to be a taking in  
6 the statute. Thus, one may convert property of the United  
7 States without intending to permanently deprive the United  
8 States of that property.

9 There is also use of the word sell; and as it is used in  
10 this particular statute it means to give or deliver or  
11 exchange property for money or its equivalent. The word  
12 convey simply means to transfer something from one to  
13 another.

14 To embezzle, as it is used in the statute, means the  
15 wrongful or willful taking of property of someone after that  
16 property has lawfully come within possession of one who has  
17 control of it.

18 The Government is not required to prove that the  
19 defendant did all of these things, that is, that the  
20 Government need not prove that he embezzled, stole or  
21 purloined and sold and conveyed the things of value that are  
22 referred to in the indictment. It is sufficient of counts 2  
23 and 4 if the Government proves beyond a reasonable doubt that  
24 the defendant did or caused one of those acts. In the  
25 absence of face value, value may be determined by looking to

1 a market value, if there would be such. If there is no  
2 market value than one for a certain Property, its value may  
3 be determined by reference to a Price that is commanded in  
4 the market Place, whether that market Place be legal or  
5 illegal. To determine the value of the exhibits you may not  
6 aggregate the value of all the exhibits to reach a total  
7 value of \$100. That is, to find the defendant guilty under  
8 counts 2 and 4 you must find the value of each one of the  
9 exhibits individually exceeds \$100.

10 All four of these counts as I have referred to them in  
11 my description of them to you used the word willfully. An  
12 act is done willfully if it is done voluntarily and  
13 intentionally and with the specific intent to do something  
14 that the law forbids. That is to say, with a bad purpose  
15 either to disobey or to disregard the law. With respect to  
16 the offenses that are charged in the indictment specific  
17 intent must be proved beyond a reasonable doubt before a  
18 defendant can be convicted. Specific intent, as that term  
19 suggests, requires more than a general intent to engage in a  
20 certain conduct. To establish specific intent the government  
21 must prove that the defendant knowingly did an act which the  
22 law forbids. It is the government's burden to present  
23 affirmative evidence of the existence of the required  
24 unlawful intent. Again, in determining whether or not the  
25 intent existed you may look at all the facts and the

1 circumstances involved in the case.

2 I referred to 4 counts in the indictment; and I would  
3 instruct you that a separate crime or offense is charged in  
4 each count, in each of the 4 counts in this case. Each  
5 charge and the evidence pertaining to it should be considered  
6 separately by you in arriving at a verdict in the case.

7 When you retire to deliberate in this case each of you  
8 should exercise your individual judgment. To return a  
9 verdict it is necessary that each of you must agree with that  
10 verdict. In other words, your verdict must be unanimous. It  
11 is your duty as jurors to consult with each other, to  
12 deliberate with a view to returning a unanimous verdict in  
13 the case if you can do so without compromising your  
14 individual opinions about the case. Each of you must decide  
15 the case for yourself, but you should not make up your mind  
16 until you have discussed the evidence with your fellow  
17 jurors. In the course of your deliberations do not hesitate  
18 to reexamine your views and change your opinion if you become  
19 convinced that your opinion is wrong, but do not surrender  
20 your honest conviction solely for the purpose of meeting your  
21 fellow jurors' consent or for the mere purpose of returning a  
22 unanimous verdict.

23 As jurors you are not partisans. Rather, you are the  
24 judges of the facts of this case. Your sole interest in the  
25 case is to ascertain the truth from the evidence that has

1 been Presented to you. There is nothing unusual about the  
2 way in which you are to consider the evidence in this case.  
3 Simply use your common sense in the light of your knowledge  
4 of the natural tendencies and the inclinations of human  
5 beings.

6 If you find the accused is guilty beyond a reasonable  
7 doubt, say so. If not, say so. Keep in mind that it would  
8 be a violation of your sworn duty to base a verdict upon  
9 anything other than the evidence in the case.

10 The Punishment that is provided for by law for the  
11 offenses that are charged in the indictment is a matter  
12 entirely within the Province of the Court. Therefore, you  
13 should not consider the possible punishment in arriving at  
14 your verdict as to the guilt or the innocence of the  
15 defendant.

16 When you retire to the jury room, juror #1, Mr. Frank  
17 Scriven (Phonetic) will act as your foreman. He will Preside  
18 over your deliberations and he will be your spokesman in  
19 Court. When you have reached a unanimous verdict, an  
20 agreement as to your verdict, you will notify the bailiff and  
21 you will then return to the courtroom with your verdict. If,  
22 during the course of your deliberations it is necessary to  
23 communicate with the Court, you may send a note with the  
24 bailiff. You should not attempt to communicate with the  
25 Court except by writing; and bear in mind always that you are

1 not to reveal to the Court or to anyone how you stand either  
2 numerically or otherwise on the question of guilt or  
3 innocence until after you have reached a unanimous verdict.

4 When you have reached a unanimous verdict you will  
5 return to the courtroom; and the clerk will then have a role  
6 call and then we will ask if you have agreed upon your  
7 verdict. You will say, we have. She will say, who shall  
8 speak for you. You will say, our foreman. Mr. Foreman, you  
9 will then stand and in response to questions asked by the  
10 clerk, how do you find the defendant as to count 1, count 2,  
11 count 3, count 4 - she will give each of them individually -  
12 you will give your verdict as to guilty or innocent as to  
13 each of those counts.

14 May I see counsel.

15 SIDEBAR CONFERENCE

16 THE COURT: Government's exceptions?

17 MR. SCHATZOW: Judge, one thing. The first time  
18 that you referred to count 1 I believe you said that count 1  
19 refers to the, also to the Naval report relating to those  
20 photos. Then the other references you made to count 1 you  
21 just said the photographs. There is no reference to a Naval  
22 report. I was wondering if you want to clarify that. It was  
23 the very first time --

24 THE COURT: Count 1 refers only to the photographs.

25 MR. SCHATZOW: Yes. Count 1 only refers to -- the

1 other --

2 THE COURT: And count 3 refers to the weekly wire.

3 MR SCHATZOW: Yes. The other 2 things. You  
4 wouldn't want to come to take back what you said about moral  
5 certainty, would you?

6 THE COURT: I didn't use the language  
7 (indiscernible)

8 MR SCHATZOW: You used the language about moral  
9 certainty --

10 THE COURT: Yes, but I did not give the definition  
11 objected to by the fourth circuit.

12 MR SCHATZOW: Right, but you used moral certainty.  
13 Want to take it back?

14 THE COURT: No.

15 MR SCHATZOW: Oh, okay. Then the other thing is  
16 you told them they couldn't aggregate the value for the  
17 photos. Want to take that back?

18 THE COURT: No.

19 MR SCHATZOW: If you would just clear up  
20 (indiscernible)

21 THE COURT: Defense objections?

22 MR MUSE: One second. It may have been a defect of  
23 my note taking, but I'm not sure that you defined it actually  
24 the way you said you were going to yesterday in terms of it  
25 not being a strain, anything reasonable or foreseeable,

1 Potentiality.

2 THE COURT: Take exception to that.

3 MR MUSE: And also just to note our exception with  
4 regard to the notion of Potential damage.

5 THE COURT: Yes.

6 MR MUSE: and (indiscernible) we Preserve our  
7 Position on it.

8 THE COURT: All right. And Your failure to grant a  
9 directed verdict.

10 MR MUSE: And finally, Your Honor, with regard to  
11 the instructions counts 4 and 1 and 3 we set forth the  
12 Particular elements that we thought the Court should give to  
13 the extent that (indiscernible) note our objection.

14 THE COURT: Okay.

15 MR MUSE: Thank You.

16 END SIDEBAR CONFERENCE

17 THE COURT: Members of the Jury, just one  
18 clarification, referring to the indictment. You will notice  
19 this rather readily from reading it. The first count refers  
20 to the Photographs and the third count refers to the weekly  
21 wine excerpts, the documents as opposed to the Photographs.

22 Members of the Jury, the time has now come for you to  
23 retire to deliberate upon your verdict. Miss Cade, will you  
24 please swear the bailiff.

25 THE CLERK: Will you come forward, please. Raise

1 Your right hand. In the Presence of almighty God do You  
2 solemnly Promise and declare that You shall well and truly  
3 Keep the jury together in some convenient room; and You shall  
4 not suffer anyone to speak to them, nor shall You speak to  
5 them Yourself unless it is to ask them whether they have  
6 agreed upon their verdict without leave of the Court.

7 THE BAILIFF: I do.

8 THE CLERK: Would You state Your name for the  
9 record.

10 THE BAILIFF: Clifton Hargadon, H A R G A D O N.

11 THE COURT: Mr. Martindale and Mr. Burden, You have  
12 been serving as alternate jurors in this case. The other 12  
13 jurors are here, Prepared to go forward with their  
14 deliberations; so You are excused from any other  
15 participation in the case. I wish to thank both of You for  
16 Your Presence and Your Patience and understanding. Do either  
17 of You have any personal objects in the jury room? Get those  
18 if You will and then come out through the door here, if You  
19 will, please. Members of the jury, the clerk will give You  
20 the exhibits and a copy of the indictment in the case. I am  
21 also going to give You the tape with the instructions I just  
22 referred, just given You. All You have to do to play this is  
23 simply plug it in, push down the forward, which is on the  
24 top, making sure it is on -- it is on start now, so just push  
25 down forward. If You want to rewind there is a rewind



1 button. If you want to stop it or if you want to fast forward  
2 they are on the top. So, that is simply the instructions I  
3 have just given you. You have it if you wish to use it.

4 (Pause)

5 THE COURT: As soon as the other 2 gentlemen come  
6 out you may retire. Wait for them.

7 (Pause)

8 THE COURT: Pat, check. They may have gone out the  
9 other door.

10 (Pause)

11 THE COURT: They've gone? Members of the jury, you  
12 may now retire to deliberate upon your verdict.

13 JURY NOT PRESENT

14 THE COURT: Gentlemen, what I would plan to do is -  
15 it is now 5:05. My practice usually is to let the jury  
16 decide what they want to do. If they should not have a  
17 verdict, as well they might not, within the next hour I plan  
18 to send a note to them saying, do you want to have dinner and  
19 continue deliberating, or do you want to go home and come  
20 back tomorrow, what do you want to do. So, why don't -- you  
21 all will be nearby, I assume.

22 MR SCHATZOW: Yes, sir. We'll be right upstairs,  
23 Your Honor.

24 THE COURT: Okay. And you all will be where?

25 MR MUSE: We'll have somebody --

1 THE COURT: Well, you will be nearby.

2 MR MUSE: Yes.

3 THE COURT: Okay, because if they should ask for  
4 anything by, in writing, I would like to be able to consult  
5 with you first.

6 MR MUSE: Could we be 5 minutes away?

7 THE COURT: All right. In any event, I would suggest  
8 you be back, if you haven't heard from me, at least by six  
9 and I'll send a note in at that time and see what their --  
10 what they want to do. Okay.

11 THE CLERK: All rise. This honorable Court is now  
12 in recess.

13 RECESS

14 (Tape turned on in middle of colloquy)

15 THE COURT: -- home. Do you want it 9:30 or 10:00?

16 MR MUSE: We're going to go back to Washington  
17 since it's early enough, so 10:00 would be preferable.

18 MR SCHATZOW: Do you want us here for the beginning  
19 of the deliberations?

20 THE COURT: Yes, sir. When the jury goes out I  
21 want you here.

22 MR SCHATZOW: Okay. Well, 10:00 is convenient for  
23 Mr Muse.

24 THE COURT: Okay. Paul.

25 OFF RECORD

1 JURY PRESENT

THE COURT: Be

2 seated, Please. Members of the jury, I understand you have  
3 reached your first decision. You want to go home. Right?

4 (Laughter)

5 THE COURT: Okay. I think, as I indicated to  
6 counsel, it is my practice to allow you all, the jurors, to  
7 decide whether you want to stay or go home. I understand a  
8 lot of reasons you may wish to go home rather than staying  
9 late and deliberating. So, what we are going to do is  
10 adjourn until tomorrow morning and ask you to come back and  
11 to continue your deliberations, but what I am going to ask  
12 you to do is this. If you come as some of you will, I'm  
13 sure, and go in the jury room, please do not discuss the case  
14 until 10:00. We'll call you into the courtroom and take a  
15 role call and then excuse you to begin your deliberations.  
16 So, if 2 or 3 of you straggle in please do not discuss the  
17 case. Do it only when all 12 of you are present. Now,  
18 there is one other problem. You will recall we had alternate  
19 jurors during the trial. Those gentlemen have now been  
20 excused, so it is up to you 12, so please be here tomorrow.  
21 Don't any of you fail to show. Okay. All right. What I am  
22 going to do is lock the jury room and have nobody come in.  
23 Nobody to empty ashtrays or clean up or anything, so there  
24 can be no repetition of what happened yesterday. It will be  
25 secure. Leave your documents out. I do suggest you put them

1 in the envelopes I think you all have. If you don't let me  
2 know and we'll have them available for you with your name on  
3 the outside. Leave them there. It will be secure. Come  
4 back in the morning so we can begin no later than 10:00. As  
5 I say, do not discuss the case until you return to the  
6 courtroom. We'll have role call and then you will return to  
7 deliberate when you are all present. Again, as I've stated  
8 before each time we have an adjournment, please do not  
9 discuss -- not please, but do not discuss the case with  
10 anyone else. Don't go home and discuss it with somebody.  
11 Don't read or listen to anything about it that may be in the  
12 printed or electronic media. Return tomorrow no later than  
13 10:00. Okay. Thank you.

14 JURY NOT PRESENT

15 THE COURT: Arthur, if you will see to it that the  
16 jurors get the elevator and get out of the building and then,  
17 in the meantime, I want to make sure that, Pat, you can make  
18 it secure, put the alarm on. Okay. Anything further,  
19 counsel? Okay. Promptly 10:00. No later than that so we  
20 can have them go out. Okay.

21 THE CLERK: All rise. This honorable court is now  
22 adjourned.

23 \*\*\*\*\*  
24  
25

1 I certify that the foregoing is a correct transcript of  
2 the Proceedings in the above-entitled matter.

3 February 12, 1966

4 *Janice Saunders*  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

GOVERNMENT PROPOSED  
MEMBER INSTRUCTIONS

Enclosure 2

21 June 2012

UNCLASSIFIED

United States v. Lieutenant Commander Matthew M. Diaz, JAG Corps, U.S. Navy

General Court-Martial

**PRELIMINARY INSTRUCTIONS ON FINDINGS**

Members of the court, when you close to deliberate and vote on the findings, each of you must resolve the ultimate question of whether the accused is guilty or not guilty based upon the evidence presented here in court and upon the instructions which I will now give you. It is my duty to instruct you on the law. Your duty is to determine the facts, apply the law to the facts, and determine the guilt or innocence of the accused, keeping in mind that the law presumes the accused to be innocent of the charges against him. At the conclusion of my instructions, I will provide a written copy to the President of the Court for your reference during deliberations.

You have just heard an exposition of the facts by counsel for both sides as they view them. Bear in mind that the arguments of counsel are not evidence. Argument is made by counsel in order to assist you in understanding and evaluating the evidence, but you must base the determination of the issues in the case on the evidence as you remember it and apply the law as I instruct you.

During the trial I noticed many of you taking notes. You may take your notes with you into the deliberation room and you may use your notes to refresh your own recollection of the evidence presented. However, your notes are not a substitute for the record of trial, and should not be shown to the other members.

You may find the accused guilty of an offense only if you are convinced as to guilt by legal and competent evidence beyond a reasonable doubt as to each and every element of that offense. I will now discuss the offenses and their elements with you in the order in which they appear on the charge sheet.

In Charge I and the sole Specification thereunder the accused is charged with the offense of:

**VIOLATION OF A GENERAL REGULATION** in violation of the UCMJ, Article 92.

In order to find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond reasonable doubt of the following:

**I. ELEMENTS**

(1) That, between on or about 20 December 2004 and 28 February 2005, there was in existence a certain lawful general regulation, to wit: Secretary of the Navy Instruction 5510.36, Navy Information Security Program, as modified by Change 1, dated 19 June 2000;

(2) That the accused had a duty to obey this regulation; and

(3) That, between on or about 20 December 2004 and 28 February 2005, at or near Guantanamo Bay, Cuba, the accused violated this lawful general regulation by wrongfully failing to properly mail classified SECRET information, by wrongfully mailing classified information.

UNCLASSIFIED

APPELLATE EXHIBIT **CXVI**  
PAGE 1 OF 19  
APPENDED PAGE 1711

UNCLASSIFIED

## II. DEFINITIONS

"General Regulations" are those orders or regulations which are generally applicable to an armed force and which are properly published by the President, the Secretary of Defense or a military department such as the Secretary of the Navy.

To be lawful, a "General Regulation" must relate to specific military duty and be one which is authorized under the circumstances. A general regulation is lawful if it is reasonably necessary to safeguard and protect the morale, discipline, and usefulness of the members of a command and is directly connected with the maintenance of good order in the services. It is illegal if it is unrelated to military duty; its sole purpose is to accomplish some private end; it is arbitrary and unreasonable; or it is given for the sole purpose of increasing the penalty for an offense which it is expected you may commit.

"Classified Information" under this charge is information that has been determined to require protection against unauthorized disclosure in the interest of national security and is classified for such purpose by appropriate classifying authority per the provisions of E.O. 12958 or any predecessor Order.

In this case, I have taken judicial notice that Secretary of the Navy Instruction 5510.36 is a lawful General Regulation. This means that you are now permitted to recognize and consider this information as fact without further proof. It should be considered by you as evidence with all other evidence in the case. You may accept as conclusive any matter I have judicially noticed, but you are not required to do so.

### Ignorance or Mistake of Fact

The evidence has raised the issue of ignorance on the part of the accused concerning the nature or status of the information that is the subject of Charge I and its specification.

Ignorance, no matter how unreasonable it might have been, is a defense to this offense. In deciding whether the accused was ignorant of the fact that the information he mailed was classified, you should consider the probability or improbability of the evidence presented on the matter.

You should consider the accused's age, education, and experience, along with the other evidence on this issue.

The burden is on the prosecution to establish the guilt of the accused. If you are convinced beyond a reasonable doubt that at the time of the alleged offense the accused was not ignorant of the fact the information he mailed was classified, then the defense of mistake does not exist.

UNCLASSIFIED

APPELLATE EXHIBIT **CXVI**  
PAGE 2 OF 14  
APPENDED PAGE 1711



In Charge II and the sole Specification thereunder, the accused is charged with the offense of:

**CONDUCT UNBECOMING AN OFFICER AND GENTLEMAN** in violation of the UCMJ, Article 133.

In order to find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond reasonable doubt of the following:

#### **I. ELEMENTS**

- (1) That, between on or about 20 December 2004 and 28 February 2005, at or near Guantanamo Bay, Cuba, the accused wrongfully and dishonorably transmitted classified documents to a person not authorized to receive them; and
- (2) That, under the circumstances, the conduct of the accused was unbecoming an officer and a gentleman.

#### **II. DEFINITIONS**

"Classified information" under this charge means any information or material that has been determined by the United States Government pursuant to an executive order, statute or regulation, to require protection against unauthorized disclosure for reasons of national security.

"Conduct unbecoming an officer and a gentleman" means behavior in an official or unofficial capacity which, in dishonoring or disgracing the individual as a commissioned officer, seriously detracts from his character as a gentleman or behavior in an unofficial or private capacity which, in dishonoring or disgracing the individual personally, seriously detracts from his standing as a commissioned officer.

Unbecoming conduct means misbehavior more serious than slight, and of a material and pronounced character. It means conduct morally unfitting and unworthy rather than merely inappropriate or unsuitable misbehavior, which is more than opposed to good taste or propriety.

#### **Ignorance or Mistake of Fact**

The evidence has raised the issue of ignorance on the part of the accused concerning the nature and status of the information that is the subject of Charge II and its specification.

Ignorance, no matter how unreasonable it might have been, is a defense to this offense. In deciding whether the accused was ignorant of the fact that the information he mailed was classified, you should consider the probability or improbability of the evidence presented on the matter. You should also consider the accused's age, education, and experience, along with the other evidence on this issue.

The burden is on the prosecution to establish the guilt of the accused. If you are convinced beyond a reasonable doubt that at the time of the alleged offense the accused was not ignorant of the fact the information he transmitted was classified, then the defense of mistake does not exist.

UNCLASSIFIED

In Charge III, Specification 1, the accused is charged with the offense of:

GATHERING NATIONAL DEFENSE INFORMATION in violation of 18 U.S.C. Sec. 793(b), a violation of the UCMJ, Article 134.

In order to find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond reasonable doubt of the following:

#### I. ELEMENTS

(1) That, between on or about 20 December 2004 and 28 February 2005, at or near Guantanamo Bay, Cuba, the accused made a "print-out" of certain information for the purpose of obtaining information respecting the national defense of the United States;

(2) That the information printed was related to the national defense of the United States;

(3) That, at the time of the printing, the accused acted with the intent or reason to believe that the information was to be used to the injury of the United States or used to the advantage of a foreign country;

#### II. DEFINITIONS

With respect to the second element, you must determine whether the information in the "print-out" was directly and reasonably connected with the national defense. The term "national defense" is a broad term which refers to the United States military and naval establishments and to all related activities of national preparedness. The information need not be classified information under security criteria, as long as you determine that the information has a reasonable and direct connection with our national defense. If, however, the information is lawfully accessible to anyone willing to take pains to find, to sift, and to collate it, you may not find that the defendant is guilty under this section. Only information relating to our national defense which is not available to the public at the time of the claimed violation falls within the prohibition of this section.

With respect to the third element, the government is required to prove that the defendant acted with criminal intent—that is, that he acted in bad faith and with a deliberate purpose either to disregard or disobey the law.

In considering whether or not the defendant had the intent that the information in the "print-out" would be used to injure the United States, or to provide an advantage to a foreign nation, you may consider the nature of the information involved. I emphasize that you must determine whether or not the defendant had the intent that the information *would* be used against the United States, not just that it *could* be so used.

The government does not have to prove that the intent was both to injure the United States and to provide an advantage to a foreign nation—the statute reads in the alternative. Further, the country to whose advantage the information would be used need not necessarily be an enemy of the United States. The statute does not distinguish between friend and enemy.

UNCLASSIFIED

UNCLASSIFIED

If you find, therefore, that the defendant acted with the intent or with reason to believe that the information would be used to injure the United States or to provide an advantage to a foreign nation, the third element of the offense is satisfied.

In Charge III, Specification 2, the accused is charged with the offense of:

**WRONGFULLY TRANSMITTING DEFENSE INFORMATION** in violation of 18 U.S.C. Sec. 793, a violation of the UCMJ, Article 134.

In order to find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond reasonable doubt of the following:

## **I. ELEMENTS**

(1) That, between on or about 20 December 2004 and 28 February 2005, at or near Guantanamo Bay, Cuba, the accused had authorized or unauthorized possession of, access to, or control over certain information;

(2) That the information was related to the national defense of the United States;

(3) That the accused had reason to believe that the information could be used to the injury of the United States or to the advantage of a foreign nation;

(4) That the accused willfully transmitted the information to a person who was not entitled to receive it.

## **II. DEFINITIONS**

The word "possession" is a commonly used and commonly understood word. Basically it means the act of having or holding property or the detention of property in one's power or command. Possession may mean actual physical possession or constructive possession. A person has constructive possession of something if he knows where it is and can get it any time he wants, or otherwise can exercise control over it.

A person has "authorized possession" of something, if he is entitled to have it.

A person has "unauthorized possession" of something, if he is not entitled to have it.

The term "national defense" has the same meaning as it does under Specification 1 of Charge III.

"Reason to believe" means that the accused knew facts from which he concluded, or reasonably should have concluded, that information he possessed could be used for the prohibited purposes. In considering whether or not the defendant had reason to believe that the information could be used to the injury of the United States, or to the advantage of another country, you may consider the nature of the information involved. It is not necessary that the accused had reason to believe the information *would* be used against the United States, only that it *could* be so used. The government does not have to prove that the defendant had reason to believe that his act could both injure the United States and be to the advantage of another country--the statute reads in the

UNCLASSIFIED

APPELLATE EXHIBIT Cxvi  
PAGE 5 OF 14  
APPENDED PAGE 1711

alternative. Also, the country to whose advantage the information could be used need not necessarily be an enemy of the United States. The statute does not distinguish between friend and enemy.

An act is done "willfully," if it is done voluntarily and intentionally with the specific intent to do something the law forbids, that is, with a bad purpose either to disobey or to disregard the law.

In deciding whether the person who received the document at issue was "entitled" to have it, you may consider all the evidence introduced at trial, including any evidence concerning the classification status of the document or testimony concerning limitations on access to the document. The government does not have to prove that the defendant communicated the documents to an agent of a foreign government. Disclosure to anyone who was not entitled to receive it is sufficient.

**In Charge III, Specification 3**, the accused is charged with the offense of:

**UNAUTHORIZED REMOVAL OF CLASSIFIED INFORMATION** in violation of 18 U.S. Code Sec. 1924, a violation of the UCMJ, Article 134.

In order to find the accused guilty of this offense, you must be convinced by legal and competent evidence beyond reasonable doubt of the following:

#### **I. ELEMENTS**

- (1) That, between on or about 20 December 2004 and 28 February 2005, at or near Guantanamo Bay, Cuba, the accused was an officer of the United States;
- (2) That by virtue of his office or position, the accused became possessed of materials containing classified information of the United States;
- (3) That the accused knowingly removed said materials;
- (4) That the accused removed said materials without authority; and
- (5) That the accused removed said materials with the intent to retain such materials at an unauthorized location.

#### **II. DEFINITIONS**

"Possession" has the same meaning as in the preceding specifications for which that term has been defined for you.

A person has possession of something "by virtue of his office" if he is authorized access or control over or otherwise encounters it in the ordinary course of his duty.

"Classified information" under this charge means information originated, owned, or possessed by the United States Government concerning the national defense or foreign relations of the

UNCLASSIFIED

United States that has been determined pursuant to law or Executive order to require protection against unauthorized disclosure in the interests of national security.

An act is done "knowingly" if it is done voluntarily and intentionally, and not because of mistake or accident or other innocent reason.

### **Ignorance or Mistake of Fact**

The evidence has raised the issue of ignorance on the part of the accused concerning the nature or status of the information that is the subject of specification 3 of Charge III.

Ignorance, no matter how unreasonable it might have been, is a defense to this offense. In deciding whether the accused was ignorant of the fact that the information he mailed was *classified*, ~~national defense information~~, you should consider the probability or improbability of the evidence presented on the matter. You should also consider the accused's age, education, and experience, along with the other evidence on this issue. *OK*

The burden is on the prosecution to establish the guilt of the accused. If you are convinced beyond a reasonable doubt that at the time of the alleged offense the accused was not ignorant of the fact the information he removed and transmitted was classified, then the defense of mistake does not exist.

## **EVIDENTIARY AND OTHER MATTERS**

### **Intent**

I have instructed you that the accused's criminal intent as to each offense must be proved beyond a reasonable doubt. Direct evidence of intent is often unavailable. The accused's intent, however, may be proven by circumstantial evidence. In deciding this issue, you must consider all relevant facts and circumstances.

### **Circumstantial Evidence**

Evidence may be direct or circumstantial. Direct evidence is evidence which tends directly to prove or disprove a fact in issue. Circumstantial evidence is evidence which tends directly to prove not a fact in issue, but some other fact or circumstance from which, either alone or together with some other facts or circumstances you may reasonably infer the existence or nonexistence of a fact in issue. There is no general rule for determining or comparing the weight to be given to direct or circumstantial evidence. You should give all the evidence the weight and value you believe it deserves.

Let me give you an example. If a witness testified that he or she saw it rain during the evening, that would be direct evidence. If there was evidence the street was wet in the morning, that would be circumstantial evidence from which you might reasonably infer that it rained during the night.

UNCLASSIFIED

APPELLATE EXHIBIT **CXVI**  
PAGE 7 OF 14  
APPENDED PAGE 1711

**Stipulation of Fact**

The parties to this trial have stipulated or agreed that Prosecution Exhibit 1 (Envelope), Prosecution Exhibit 2 (Valentine's Day Card) and Prosecution Exhibit 3 (JDIMS Report) were mailed via 1<sup>st</sup> Class Mail from the Post Office on board the U.S. Naval Station in Guantanamo Bay, Cuba, and had a post-mark date of 15 January 2005.

When counsel for both sides, with the consent of the accused, stipulate and agree to a fact, the parties are bound by the stipulation and the stipulated matters are facts in evidence to be considered by you along with all the other evidence in the case.

**Judicial Notice**

I have taken judicial notice that the following were lawful general regulations, directives or guidance documents, in effect in January 2005:

Secretary of the Navy Instruction 5510.36, dated 17 March 1999, as modified by change 1 dated 19 June 2000;

Executive Order 12958, 3 C.F.R. Sec. 333 (1995), as amended by Executive Order 13292 (March 25, 2003), reprinted as amended in 50 U.S.C. Sec. 435 (2007);

Information Security Oversight Office Implementing Directive No. 1 (effective September 22, 2003);

Department of Defense Guide to Marking Classified Documents, DoD 5200.1-PH (April 1997);

Department of Defense Regulation 5200.1-R, Department of Defense Information Security Program, dated January 1997.

This means that you are now permitted to recognize and consider this fact without further proof. It should be considered by you as evidence with all other evidence in the case. You may, but are not required to, accept as conclusive any matter I have judicially noticed.

**Credibility of Witnesses**

You have the duty to determine the believability of the witnesses. In performing this duty you must consider each witness' intelligence, ability to observe and accurately remember, and the witness' sincerity and conduct in court.

Consider also the extent to which each witness is either supported or contradicted by other evidence; the relationship each witness may have with either party to this case; and how each witness might be affected by the verdict. In weighing a discrepancy or discrepancies by a witness or between witnesses, you should consider whether it or they resulted from an innocent mistake or a deliberate lie.

Taking all these matters into account, you should then consider the probability of each witness' testimony and the inclination of the witness to tell the truth.

UNCLASSIFIED

The believability of each witness' testimony should be your guide in evaluating testimony and not the number of witnesses called.

### Expert Testimony

You have heard the testimony of a number of expert witnesses in this case: Mr. Paul Rester, an expert in interrogations and classification of information, Ms. Lynda Strong and Ms. Alison Rees, forensic fingerprint examiners, Mr. Robert Kates and Mr. Joshua Homan, experts in computer networks and databases. These individuals are known as expert witnesses because their knowledge, skill, experience, training, or education may assist you in understanding the evidence or in determining a fact in issue. You are not required to accept the testimony of an expert witness or to give it more weight than the testimony of an ordinary witness. You should, however, consider their qualifications as experts in their respective fields.

### Good Military Character Evidence

To show the probability of the accused's innocence, the defense has produced evidence of the accused's good military character, his good military record while serving on active duty in the United States, and his law-abiding character.

Evidence of the accused's good character may, alone or in combination with other evidence, be sufficient to cause a reasonable doubt as to his guilt. On the other hand, evidence of the accused's good military character and good military record, and his law abiding character, may be outweighed by other evidence tending to show the accused's guilt. That determination is solely for you to make as the finders of fact in this case.

### "Spill-over"

An accused may be convicted of a charge based only on evidence before the court. So, each offense must stand on its own and you must keep the evidence of each offense separate. Stated differently, if you find or believe that the accused is guilty of one offense, you may not use that finding or belief as a basis for inferring, assuming, or proving that he committed any other offense.

However, if evidence has been presented which is relevant to more than one offense, you may consider that evidence with respect to each offense to which it is relevant.

The burden is on the prosecution to prove each and every element of each offense beyond a reasonable doubt. Proof of one offense carries with it no inference that the accused is guilty of any other offense. Similarly, you may not infer that the accused is guilty of any charged offense because you believe that he may have committed another offense that is not listed on the charge sheet.

### Other Conduct

You may consider Prosecution Exhibit 17, Security In Brief/Out Brief, Prosecution Exhibit 30, General Order #2, and Prosecution Exhibit 31, Policy Memorandum #8, and the testimony of Ms. Lorie Bobzein regarding these exhibits as evidence that the accused may have participated in

UNCLASSIFIED

APPELLATE EXHIBIT **OKVI**  
PAGE 9 OF 14  
APPENDED PAGE 1711



**UNCLASSIFIED**

and signed a security in-brief and out-brief. You may also consider this evidence for its tendency, if any, to prove knowledge on the part of the accused regarding the policies and requirements that were the subject of the briefs, including General Order #2 and Policy Memorandum #8.

You may not consider this evidence for any other purpose, and you may not conclude from this evidence that the accused is a bad person or has general criminal tendencies and that he, therefore committed the offenses charged.

#### **Accused's Right Not To Testify**

The accused has an absolute right to remain silent. You will not draw any inference adverse to the accused from the fact that he did not testify as a witness. The fact that the accused has not testified must be totally disregarded by you.

#### **Closed Sessions**

You may not infer that the accused is guilty of any offense from the use of a particular classification marking on an item of evidence, or the presentation of evidence in closed trial sessions. You also may not infer from the classification markings, security precautions, or the fact that two sessions of the trial were closed to the public, that the evidence or testimony presented was either true or was in fact classified.

You must evaluate open and closed session evidence and witnesses using the same standards.

Classified evidence also does not permit any inference as to the guilt of the accused. You may not infer from the fact that the evidence was presented in a closed trial session that the accused knew the evidence was classified or that it related to the national defense of the United States.

Again, closed trial sessions to consider purportedly classified evidence are the most satisfactory method for resolving the competing needs of the Government for protection of the purportedly classified information and the rights of the accused to a public trial. You may not hold the fact there have been closed trial sessions in any way against the accused. Closed trial sessions do not erode the presumption of innocence which the law guarantees the accused.

#### **CLOSING SUBSTANTIVE INSTRUCTIONS ON FINDINGS and PROCEDURAL INSTRUCTIONS ON FINDINGS**

You are further advised:

First, that the accused is presumed to be innocent until his guilt is established by legal and competent evidence beyond a reasonable doubt;

Second, if there is reasonable doubt as to the guilt of the accused, that doubt must be resolved in favor of the accused, and he must be acquitted; and

**UNCLASSIFIED**

APPELLATE EXHIBIT CVI  
PAGE 10 OF 14  
APPENDED PAGE 1711



Third, if there is a reasonable doubt as to the degree of guilt, that doubt must be resolved in favor of the lower degree of guilt as to which there is no reasonable doubt;

### **Reasonable Doubt**

The burden of proof to establish the guilt of the accused beyond a reasonable doubt is on the government. The burden never shifts to the accused to establish innocence or to disprove the facts necessary to establish each element of each offense.

Some of you may have served as jurors in civil cases, or as board members in administrative boards, where you were told that it is only necessary to prove that a fact is more likely true than not true. In criminal cases, the government's proof must be more powerful than that. It must be beyond a reasonable doubt.

By reasonable doubt is intended not a fanciful or ingenious doubt or conjecture, but an honest, conscientious doubt suggested by the material evidence or lack of it in this case. It is an honest misgiving generated by insufficiency of proof of guilt. Proof beyond a reasonable doubt means proof to an evidentiary certainty although not necessarily to an absolute or mathematical certainty. The proof must be such as to exclude not every hypothesis or possibility of innocence, but every fair and rational hypothesis except that of guilt.

The rule as to reasonable doubt extends to every element of the offense, although each particular fact advanced by the prosecution, which does not amount to an element, need not be established beyond a reasonable doubt. However, if, on the whole evidence, you are satisfied beyond a reasonable doubt of the truth of each and every element, then you should find the accused guilty.

### **Credibility of Witnesses**

You should bear in mind that only matters properly before the court as a whole should be considered. In weighing and evaluating the evidence you are expected to utilize your own common sense, your knowledge of human nature and the ways of the world. In light of all the circumstances in the case, you should consider the inherent probability or improbability of the evidence. Bear in mind you may properly believe one witness and disbelieve several other witnesses whose testimony is in conflict with the one. The final determination as to the weight or significance of the evidence and the credibility of the witnesses in this case rests solely upon you.

### **Member Expertise**

This case involves issues about classified information and the use of computer systems, networks and software. Among you there are varying levels of familiarity with computers, software, networks and classified information. You may all consider your everyday knowledge of these matters in evaluating the evidence in this case, because such knowledge is now common among officers of your grade and experience in the Navy. You are cautioned, however, that no member may use personal expertise beyond such common knowledge in reaching his or her own conclusions, or in persuading other members during deliberations.

### Comments of Military Judge

You must disregard any comment or statement or expression made by me during the course of the trial that might seem to indicate any opinion on my part as to whether the accused is guilty or not guilty, since you alone have the responsibility to make that determination. Each of you must impartially decide whether the accused is guilty or not guilty in accordance with the law I have given you, the evidence admitted in court, and your own conscience.

### Comments of Counsel

If counsel have made reference in their closing arguments to instructions that I will give you, I would merely say that if there is any inconsistency between what counsel have said about the instructions and the instructions which I gave you, you must accept my statement as being correct. In addition, you must not consider adversely to either party the fact that counsel for that party, in the proper discharge of their responsibilities, made an objection.

### Findings with a Variance

If you have doubt about the time, place, or manner in which any of the alleged acts described in the specifications occurred, but you are satisfied beyond a reasonable doubt that the offense, was committed at a time, at a place, or in a particular manner, which differs slightly from that alleged in the specifications, you may make minor modifications in reaching your findings by changing the time, place, or manner in which the alleged offenses described in the specification occurred, provided that you do not change the nature or identity of the offense. You do this by making appropriate exceptions and substitutions to the specification as necessary to properly reflect your findings.

For example, in the event that you find the accused guilty of Charge III, specification 2, you must have determined beyond a reasonable doubt that the accused had either "authorized" or "unauthorized" access to national defense information. If you determine that the accused had authorized or unauthorized access to national defense information, you must indicate that fact in any finding of guilty to Charge III, specification 2, by indicating on the findings worksheet that you find the accused guilty "except the word authorized" or "except the word unauthorized."

Your findings worksheet has been drafted in a manner that will allow you to make findings by exceptions, or by exceptions and substitutions, if you believe it is appropriate to accurately record your findings.

### Procedural Instructions

The following procedural rules will apply to your closed session deliberations and must be strictly observed: The influence of superiority in rank will not be employed in any manner in an attempt to control the independence of the members in the exercise of their own personal judgment. Your deliberation should include a full and free discussion of all the evidence that has

UNCLASSIFIED

been presented. After you have completed your discussion, then voting on your findings must be accomplished by secret, written ballot, and all members of the court are required to vote.

The order in which the several charges and specifications are to be voted on should be determined by the president subject to objection by a majority of the members. You vote on the specification under the charge before you vote on the charge. If you find the accused guilty of a specification under a charge, the finding as to that charge must be guilty. The junior member will collect and count the votes. The count will then be checked by the president, who will immediately announce the result of the ballot to the members.

The concurrence of at least two-thirds of the members present when the vote is taken is required for any finding of guilty. Since we have 7 members, that means 5 members must concur in any finding of guilty. If you have at least 5 votes of guilty of any offense, then that will result in a finding of guilty for that offense. If fewer than 5 members vote for a finding of guilty, then your ballot resulted in a finding of not guilty.

You may reconsider any finding prior to its being announced in open court. However, after you vote, if any member expresses a desire to reconsider any finding, you are instructed to open the court and the President should announce only that reconsideration of a finding has been proposed. Do not state:

- (1) whether the finding proposed to be reconsidered is a finding of guilty or not guilty, or
- (2) which specification and charge is involved. I will then give you specific further instructions on the procedure for reconsideration.

As soon as the court has reached its findings, and I have examined the Findings Worksheet, the findings will be announced by the President in the presence of all parties. As an aid in putting your findings in proper form and making a proper announcement of the findings, you may use Appellate Exhibit CV, the Findings Worksheet, which the Bailiff may now hand to the President.

Captain Zintz, please look at Appellate Exhibit CV and note that the first section will be used if the accused is completely acquitted of all charges and specifications. The second section will be used if the accused is convicted of one or more, or all the offenses. As I previously noted, it might be necessary for you to record findings that vary from the language charged in Charge III, specification 2. The second section of the findings worksheet has been drafted to assist you in recording those findings. The third section is provided to assist you in making findings by exceptions and substitutions as to any other specification. Finally, once you have recorded your findings, please line through every unused section and all unused language within a section used, and fill in any applicable blanks. This will allow me to readily check your findings and ensure that they are in proper form.

The worksheet is provided only as an aid in finalizing your decision.

If, during your deliberations, you have any questions, open the court, and I will assist you.

UNCLASSIFIED

APPELLATE EXHIBIT **CXVI**  
PAGE 13 OF 14  
APPENDED PAGE 1711

**UNCLASSIFIED**

The Uniform Code of Military Justice prohibits me and everyone else from entering your closed session deliberations. You may not consult the Manual for Courts-Martial or any other legal publication, unless it has been admitted into evidence.

If it is necessary, your deliberations may be interrupted by a recess. However, before you may leave your closed session deliberations, you must notify me, we must come into the courtroom, formally convene and then recess the court. Then, after the recess, we must reconvene the court, and formally close again for your deliberations. This is a vital legal requirement. So, with that in mind, Captain Zintz, do you want to take a brief recess before you begin your deliberations, or would you like to begin immediately?

Bailiff, please provide Captain Zintz the folders containing all Prosecution Exhibits and Defense Exhibits for use during the court's deliberations. Captain Zintz, let me remind you that those exhibits include information that is marked classified and must remain in your control until returned to the Bailiff when you return to an open session of court.

Finally, Members, please do not mark on any of the exhibits, except the Findings Worksheet and Captain Zintz, please bring all the exhibits with you when you return to announce your findings.

**UNCLASSIFIED**

APPELLATE EXHIBIT **CXVI**  
PAGE 14 OF 14  
APPENDED PAGE 1711

) ) ) ) ) ) ) ) ) )

)

)  
 )  
 )  
 )  
 )

**21 June 2012**

## Federal Jury Practice And Instructions

Manual of Model Criminal Jury Instructions for the District Courts of the Eighth Circuit  
Prepared by Judicial Committee on Model Jury Instructions For the Eighth Circuit

## 6.00. Final Instructions: Elements of Offenses

## 6.18.641 Theft of Government Money or Property ( 18 U.S.C. § 641)

The crime of theft of Government [property]<sup>1</sup> as charged in the indictment has three elements which are:

*One*, the defendant voluntarily, intentionally and knowingly [embezzled] [stole] [converted] [money] [thing of value]<sup>2</sup> [to [his] [her] [their] own use or to the use of another]; and

*Two*, the [money] [thing of value]<sup>3</sup> belonged to the United States and had a value in excess of One Thousand Dollars (\$1,000);<sup>4</sup> and

*Three*, the defendant did so with intent to deprive the owner of the use or benefit of the [money] [thing of value]<sup>5</sup> or property so taken.

The word "value" means the face, par, or market value, or cost price, either wholesale or retail, whichever is greater.<sup>6</sup>

A "thing of value" can be tangible or intangible property.<sup>7</sup>

It is not necessary to prove that the defendant knew that the Government owned the property at the time of the wrongful taking so long as it is established, beyond a reasonable doubt, that the Government did in fact own the money or property involved, that it had a value in excess of One Thousand Dollars (\$1,000), and that the defendant knowingly and willfully [embezzled] [stole] [converted] it.

[To "embezzle" means voluntarily and intentionally to take or to convert to one's use the property of another which property came into the defendant's possession lawfully.]

(Insert paragraph describing Government's burden of proof; see Instruction 3.09, *supra*.)

## Notes on Use

1., 2., 3., 5. The statute covers "record," "voucher," "money," "thing of value," or "property made or being made under [federal] contract." Whichever form is applicable should be used.

4. The statute provides for both a felony offense and a misdemeanor offense. Section 641 was amended by section 606 of The Economic Espionage Act of 1996, Pub. L. 104-294, 110 Stat. 3511, to make value in excess of \$1,000 the felony threshold. The Committee recommends that the jury specifically find that the amount embezzled or misapplied exceeded \$1,000. If this issue is controverted, the misdemeanor offense should be included in the instructions as a lesser-included offense. Alternatively, a special interrogatory could be submitted

to the jury asking it whether it finds, beyond a reasonable doubt, that the item had a value of more than \$1,000 at the time of the alleged offense.

**6. 18 U.S.C. § 641.**

7. *United States v. May*, 625 F.2d 186, 190–91 (8th Cir. 1980). *See also United States v. DiGilio*, 538 F.2d 972 (3d Cir. 1976) (copying F.B.I. documents and selling the copies held to violate the statute) and *United States v. Morison*, 604 F. Supp. 655, 663–64 (D. Md. 1985), *aff'd*, 844 F.2d 1057 (4th Cir. 1988) (statute applied to unauthorized disclosures of classified information).

**Committee Comments**

*See United States v. Walker*, 563 F. Supp. 805 (S.D. Iowa 1983).

The Committee believes that the intent required by 18 U.S.C. § 641 is adequately covered by Elements One and Three. *United States v. May*, 625 F.2d 186 (8th Cir. 1980); *United States v. Denmon*, 483 F.2d 1093 (8th Cir. 1973).

In this statute, steal or stealing has been given broader meaning than larceny at common law. The statute applies to any taking whereby a person dishonestly obtains anything of value belonging to another with the intent to deprive the owner of the rights and benefits of ownership. *Crabb v. Zerbst*, 99 F.2d 562 (5th Cir. 1938). *See also Morissette v. United States*, 342 U.S. 246, 267–69 n.28 (1952).

FEDCRIM-JI8C 6.18.641

END OF DOCUMENT

) ) ) ) ) ) ) ) ) )

**V.**

**Manning, Bradley E.**  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

**Enclosure 4**

21 June 2012



Federal Jury Practice And Instructions  
Pattern Jury Instructions: Fifth Circuit, Criminal Cases  
Prepared by the Committee on Pattern Jury Instructions District Judges Association Fifth Circuit

II. Substantive Offense Instructions

2.33 Theft of Government Money or Property

18 U.S.C. § 641 (First Paragraph)

Title 18, United States Code, Section 641, makes it a crime for anyone to embezzle [steal] [convert] any money or other property belonging to the United States having a value of more than \$1,000.

For you to find the defendant guilty of this crime, you must be convinced that the government has proved each of the following beyond a reasonable doubt:

*First:* That the money or property described in the indictment, \_\_\_\_\_, [describe property] belonged to the United States government and had a value in excess of \$1,000 at the time alleged;

*Second:* That the defendant embezzled [stole] [converted] such money [property] to the defendant's own use [to the use of another]; and

*Third:* That the defendant did so knowing the property was not his, and with intent to deprive the owner of the use [benefit] of the money [property].

The word "value" means the face, par, or market value, or cost price, either wholesale or retail, whichever is greater.

It is not necessary to prove that the defendant knew that the United States government owned the property at the time of the wrongful taking.

[To "embezzle" means the wrongful, intentional taking of money or property of another after the money or property has lawfully come within the possession or control of the person taking it.]

[To "steal" or "convert" means the wrongful taking of money or property belonging to another with intent to deprive the owner of its use or benefit either temporarily or permanently. Any appreciable change of the location of the property with the intent to deprive constitutes a stealing whether or not there is an actual removal of it from the owner's premises.]

No particular type of movement or carrying away is required to constitute a "taking."

Note

See *United States v. Aguilar*, 967 F.2d 111 (5th Cir.1992), quoting portions of the instruction. For a discussion of whether federal funds given to state programs retain their federal character, see *United States v. Long*, 996 F.2d 731 (5th Cir.1993).

See *United States v. Sanders*, 793 F.2d 107 (5th Cir.1986) (clothing that employee of Army and Air Force Exchange Service sought to remove from exchange premises without paying for it constituted a "thing of value of the United States within the meaning of the statute"); *United States v. Barnes*, 761 F.2d 1026 (5th Cir.1985) (government does not have to prove that it suffered actual property loss in a § 641 prosecution, declining to follow dictum in *United States v. Evans*, 572 F.2d 455 (5th Cir.1978), *cert. denied*, 99 S.Ct. 200 (1978)).

If a disputed issue is whether the property stolen had a value of more than \$1,000, the court should consider giving a lesser included offense instruction.

FEDCRIM-J15C 2.33

END OF DOCUMENT

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

GOVERNMENT PROPOSED  
MEMBER INSTRUCTIONS

Enclosure 5

21 June 2012

Federal Jury Practice And Instructions  
Current through November 2010

Ninth Circuit Manual of Model Jury Instructions -- Criminal  
Committee on Model Jury Instructions Ninth Circuit

8. Offenses Under Title 18

**8.95 Obtaining Information by Computer—Injurious to United States or Advantageous to Foreign Nation  
(18 U.S.C. § 1030( a)( 1) )**

The defendant is charged in [Count \_\_\_\_\_ of] the indictment with obtaining and transmitting injurious information by computer in violation of Section 1030( a)( 1) of Title 18 of the United States Code. In order for the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, the defendant knowingly [accessed without authorization] [exceeded authorized access to] a computer;

Second, by [accessing without authorization] [exceeding authorized access to] a computer, the defendant obtained [information that had been determined by the United States government to require protection against disclosure for reasons of national defense or foreign relations] [data regarding the design, manufacture or use of atomic weapons];

Third, the defendant had reason to believe that the information or data obtained could be used to the injury of the United States or to the benefit of a foreign nation; and

[Fourth, the defendant willfully [caused to be] [[communicated] [delivered] [transmitted]] the information or data to any person not entitled to receive it.]

*or*

[Fourth, the defendant willfully [caused to be] retained and failed to deliver the information or data to an officer or employee of the United States entitled to receive it.]

**Comment**

18 U.S.C. § 1030(e) provides definitions of the terms “computer,” “exceeds authorized access,” and “person.” As to “knowingly,” *see* Instruction 5.6 (Knowingly—Defined), and as to “willfully,” *see* Comment in 5.5 (Willfully).

FEDCRIM-JI9C 8.95

END OF DOCUMENT

)  
)  
)  
)  
)  
)  
)  
)

Y.

**Manning, Bradley E.**  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

## GOVERNMENT PROPOSED MEMBER INSTRUCTIONS

**Enclosure 6**

**21 June 2012**

# MODERN FEDERAL JURY INSTRUCTIONS

---

VOLUME 1

*HON. LEONARD B. SAND  
JOHN S. SIFFERT  
WALTER P. LOUGHLIN  
STEVEN A. REISS  
STEVE ALLEN  
HON. JED S. RAKOFF*

2011

*Filed Through:*  
**RELEASE NO. 59B, NOVEMBER 2011**



LexisNexis®

## QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please call:

Mark A. Landis, J.D. at ..... 1-415-908-3300

Email: ..... Mark.A.Landis@lexisnexis.com

Benjamin Speaker at ..... 1-908-673-3391

Email: ..... Benjamin.H.Speaker@lexisnexis.com

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844

Outside the United States and Canada, please call ..... (518) 487-3000

Fax Number ..... (518) 487-3584

For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940

Outside the United States and Canada, please call ..... (518) 487-3000

Library of Congress Card Number: 84-072026

ISBN: 978-0-8205-1485-7

Cite as:

[Vol. #]-[Ch. #] *Modern Federal Jury Instructions-Criminal*, ¶ [000.00] (Matthew Bender)

Example:

2-71 *Modern Federal Jury Instructions-Criminal*, ¶ 71.01 (Matthew Bender)

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks and Michie is a trademark of Reed Elsevier Properties Inc., used under license. Matthew Bender and the Matthew Bender Flame Design are registered trademarks of Matthew Bender Properties Inc.

Copyright © 2011 Matthew Bender & Company, Inc., a member of the LexisNexis Group.

Originally published in 1984

All Rights Reserved.

No copyright is claimed in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material exceeding fair use, 17 U.S.C. § 107, may be licensed for a fee of 25¢ per page per copy from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

Editorial Offices  
121 Chantlot Rd., New Providence, NJ 07974 (908) 464-6800  
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200  
www.lexisnexis.com

MATTHEWBENDER

(Rel 59B: 11/2011 Pub 485)

# Modern Federal Jury Instructions

CRIMINAL

SAMUEL STEPHEN LOUGHLIN  
REID ALLEN RAKOFF



1975

CELESTINE 1 - 23



3 5127 00213 6695

KF  
9682  
A65  
M64  
1984  
v. 1: Criminal  
inal

# Modern Federal Jury Instructions

CRIMINAL

8/100 10/1000000 - 10/1000000  
RE 10/1000000 10/1000000

## CHAPTER 29

### Espionage

#### Synopsis

- ¶ 29.01. Gathering Defense Information (18 U.S.C. § 793(a))
- Instruction 29-1: The Indictment and the Statute
  - Instruction 29-2: Purpose of the Statute
  - Instruction 29-3: Elements of the Offense
  - Instruction 29-4: First Element—Defendant “Went Upon” Vessel or Place
  - Instruction 29-5: Second Element—Information Related to National Defense
  - Instruction 29-6: Third Element—Knowledge and Intent
- ¶ 29.02. Gathering Defense Information (18 U.S.C. § 793(b))
- Instruction 29-7: The Indictment and the Statute
  - Instruction 29-8: Purpose of the Statute
  - Instruction 29-9: Elements of the Offense
  - Instruction 29-10: First Element—Defendant Copied a Document
  - Instruction 29-11: Second Element—Information Related to National Defense
  - Instruction 29-12: Third Element—Knowledge and Intent
- ¶ 29.03. Gathering Defense Information (18 U.S.C. § 793(c))
- Instruction 29-13: The Indictment and the Statute
  - Instruction 29-14: Purpose of the Statute
  - Instruction 29-15: Elements of the Offense
  - Instruction 29-16: First Element—Defendant Received or Obtained a Document
  - Instruction 29-17: Second Element—Information Related to National Defense
  - Instruction 29-18: Third Element—Knowledge and Intent
- ¶ 29.04. Gathering Defense Information (18 U.S.C. § 793(d) & (e))
- Instruction 29-19: The Indictment and the Statute
  - Instruction 29-20: Purpose of the Statute
  - Instruction 29-21: Elements of the Offense

FEDERAL JURY INSTRUCTIONS

29-2

- Instruction 29-22:** First Element—Possession
- Instruction 29-23:** Second Element—Information Related to National Defense
- Instruction 29-24:** Third Element—Information Could Be Used To Prejudice of the United States
- Instruction 29-25:** Fourth Element—Defendant Willfully Delivered Information to Person Not Entitled To Receive It

## ¶ 29.04. Gathering Defense Information (18 U.S.C. § 793(d) &amp; (e))

## Instruction 29-19

## The Indictment and the Statute

The indictment charges the defendant with the illegal gathering of defense information. The indictment reads as follows:

## {Read Indictment}

The indictment charges the defendant with violating section 793(d) (or (e)) of Title 18 of the United States Code, which provides:

(d) Whoever, lawfully having possession of . . . any document . . . relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, . . . the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it [commits a crime].

(e) Whoever having unauthorized possession of . . . any document . . . relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, . . . the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it [commits a crime].

Instruction 29-20

Purpose of the Statute

Protection of the military secrets of the United States is crucial to the security of the United States and to its people. Congress, therefore, has made it a crime to jeopardize the security of the United States by gathering, transmitting, delivering or attempting to gather, transmit, or deliver information pertaining to the national defense.

Instruction 29-21  
Elements of the Offense

In order to establish a violation of section 793(d) (*or* (e)), the government must prove all of the following elements beyond a reasonable doubt:

First, that the defendant had lawful (*or* unauthorized) possession of (*or* access to *or* control over) [describe document].

Second, that the [document] was related to the national defense.

Third, that the defendant had reason to believe that the document could be used to the injury of the United States or to the advantage of [name of foreign country].

Fourth, that on [insert date], the defendant willfully communicated (*or* delivered *or* transmitted *or* caused to be communicated, delivered, or transmitted *or* attempted to communicate, deliver or transmit) the document to [name of person], who was not entitled to receive it.

Authority

Ninth Circuit: United States v. Lee, 584 F.2d 980 (9th Cir. 1979).



## Instruction 29-22

## First Element—Possession

The first element of the offense which the government must prove beyond a reasonable doubt is that the defendant had (*either lawful or unauthorized*) possession of (*or control over or access to*) [describe document].

The word "possession" is a commonly used and commonly understood word. Basically it means the act of having or holding property or the detention of property in one's power or command. Possession may mean actual physical possession or constructive possession. A person has constructive possession of something if he knows where it is and can get it any time he wants, or otherwise can exercise control over it.

*In section 793(d) cases:* A person has lawful possession of something if he is entitled to have it.

*In section 793(e) cases:* A person has unauthorized possession of something if he is not entitled to have it.

## Authority

**Fifth Circuit:** *United States v. Sink*, 586 F.2d 1041 (5th Cir. 1978), *cert. denied*, 443 U.S. 912 (1979).

**Tenth Circuit:** *United States v. Zink*, 612 F.2d 511 (10th Cir. 1980).

---

Comment

The only difference between the act proscribed in section 793(d) and that proscribed in section 793(e) is that, in section 793(d), the defendant must have had lawful possession, whereas in section 793(e) such possession must have been unauthorized. The recommended instructions reflect this difference.

## Instruction 29-23

Second Element—Information Related to National Defense<sup>1</sup>

The second element of the offense which the government must prove beyond a reasonable doubt is that the [document] is connected with the national defense of the United States.

You must determine whether the [document] is directly and reasonably connected with the national defense. The term "national defense" is a broad term which refers to United States military and naval establishments and to all related activities of national preparedness. The information need not be classified information under security criteria as long as you determine that the information has a reasonable and direct connection with our national defense. If, however, the information is lawfully accessible to anyone willing to take pains to find, to sift, and to collate it, you may not find that the defendant is guilty of espionage under this section. Only information relating to our national defense which is not available to the public at the time of the claimed violation falls within the prohibition of this section.

## Authority

United States Supreme Court: *Gorin v. United States*, 312 U.S. 19, 61 S. Ct. 429, 85 L. Ed. 488 (1941).

Second Circuit: *United States v. Soblen*, 301 F.2d 236 (2d Cir. 1962).

---

Comment

*See* Comment to Instruction 29-5, *above*.

<sup>1</sup> Adapted from the charge of Judge Weinfeld in *United States v. Drummond*, 63 Cr. 910 (S.D.N.Y. 1963).

## Instruction 29-24

Third Element—Information Could Be Used To Prejudice of the United States<sup>1</sup>

The third element of the offense which the government must establish beyond a reasonable doubt is that the defendant had reason to believe that the [document concerned] could be used to the injury of the United States or to the advantage of [name of country].

“Reason to believe” means that the defendant knew facts from which he concluded or reasonably should have concluded that the [document concerned] could be used for the prohibited purposes. In considering whether or not the defendant had reason to believe that the [document concerned] could be used to the injury of the United States, or to the advantage of [name of country], you may consider the nature of the information involved. You need not determine that the defendant had reason to believe that the [document concerned] *would* be used against the United States, only that it *could* be so used.

The government does not have to prove that the defendant had reason to believe that his act could both injure the United States and be to the advantage of [name of country]—the statute reads in the alternative. Also, the country to whose advantage the information could be used need not necessarily be an enemy of the United States. The statute does not distinguish between friend and enemy.

## Authority

**United States Supreme Court:** *Gorin v. United States*, 312 U.S. 9, 61 S. Ct. 411, 85 L. Ed. 488 (1941).

**Fourth Circuit:** *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980).

**Ninth Circuit:** *United States v. Lee*, 584 F.2d 980 (9th Cir. 1979).

## Comment

A possible explanation of the congressional purpose in establishing a lesser standard of proof regarding the defendant's belief in paragraphs (d) and (e) may be that the offenses described in those paragraphs, unlike those in paragraphs (a) and (b), involve an actual or attempted willful disclosure or retention of information relating to the national defense.<sup>2</sup>

<sup>1</sup> Adapted from the charge of Judge Weinfeld in *United States v. Drummond*, 63 Cr. 910 (S.D.N.Y. 1963).

<sup>2</sup> *United States v. Perkins*, 47 C.M.R. 259 (C.M.A. 1973).

## Instruction 29-25

**Fourth Element—Defendant Willfully Delivered Information to Person  
Not Entitled To Receive It**

The fourth element of the offense which the government must establish beyond a reasonable doubt is that the defendant willfully communicated (*or delivered or transmitted or caused to be communicated, delivered, or transmitted or attempted to communicate, deliver, or transmit*). [document concerned] to [person to whom document communicated/delivered/transmitted], who was not a person entitled to receive it.

In deciding whether the person who received the document at issue was entitled to have it, you may consider all the evidence introduced at trial, including any evidence concerning the classification status of the document or testimony concerning limitations on access to the document. (*If appropriate*: The government does not have to prove that the defendant communicated the documents to an agent of a foreign government. Disclosure to anyone who was not entitled to receive it is sufficient.)

An act is done willfully if it is done voluntarily and intentionally and with the specific intent to do something the law forbids, that is to say, with a bad purpose either to disobey or disregard the law.

The government need not prove that the defendant actually delivered [document concerned]—it is enough to prove that the defendant merely attempted to do so. Further, the government need not prove that the defendant did the act himself—it is enough to prove that he merely caused the act to be done.

**Authority**

**Fourth Circuit:** United States v. Morison, 844 F.2d 1057 (4th Cir.), *cert. denied*, 488 U.S. 908 (1988).

**Ninth Circuit:** United States v. Lee, 584 F.2d 980 (9th Cir. 1979).

---

**Comment**

The instruction must be modified accordingly when the offense charged is that the defendant refused to deliver a document to one who was entitled to receive it.

As the optional language in the Instruction indicates, there is no requirement that defendant disclose the classified information to an agent of a foreign

government.<sup>1</sup> Thus, the Fourth Circuit held that disclosure of classified photographs to a news organization satisfied this element.<sup>2</sup>

<sup>1</sup> United States v. Morison, 844 F.2d 1057, 1070h Cir.), *cert. denied*, 488 U.S. 908 (1988) (section 793(d) not limited to "classic spying").

<sup>2</sup> *Id.* at 1073-74.

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

GOVERNMENT PROPOSED  
MEMBER INSTRUCTIONS

Enclosure 7

21 June 2012

IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA  
Alexandria Division

|                           |   |                  |
|---------------------------|---|------------------|
| UNITED STATES OF AMERICA, | ) |                  |
|                           | ) |                  |
| Plaintiff,                | ) | CR. NO. 01-405-A |
|                           | ) |                  |
| vs.                       | ) |                  |
|                           | ) |                  |
| BRIAN PATRICK REGAN,      | ) |                  |
|                           | ) |                  |
| Defendant.                | ) |                  |

TRIAL TRANSCRIPT  
February 10, 2003

---

BEFORE: THE HONORABLE GERALD BRUCE LEE  
UNITED STATES DISTRICT JUDGE

APPEARANCES:

FOR THE GOVERNMENT: OFFICE OF THE UNITED STATES ATTORNEY  
BY: PATRICIA HAYNES, ESQ.  
Page 1

Regan Trial Feb 10 2003 (Instructions)  
JAMES GILLIS, ESQ.  
STEPHEN DOYLE, ESQ.  
2100 Jamieson Ave.  
Alexandria, Virginia 22314

FOR THE DEFENDANT: DIMURO GINSBERG & MOOK, PC  
BY: NINA J. GINSBERG, ESQ.  
908 King Street  
Suite 200  
Alexandria, VA 22314

LAW OFFICES OF JONATHAN SHAPIRO  
BY: JONATHAN SHAPIRO, ESQ.  
910 King Street  
Alexandria, VA 22314

DELANEY MCCARTHY & COLTON, PC  
BY: JOSEPH J. MCCARTHY, ESQ.  
510 King Street  
Suite 400  
Alexandria, VA 22314

LAND, CLARK, CARROLL &  
MENDELSON, PC  
BY: JAMES C. CLARK  
112 South Alfred Street  
Suite 300  
Alexandria, VA 22320

---

OFFICIAL COURT REPORTER: RENECIA A. SMITH-WILSON, RMR  
U.S. District Court  
401 Courthouse Square, 5th Floor  
Alexandria, VA 22314  
(703)549-5322

INDEX

|   |                    |        |
|---|--------------------|--------|
| 1 |                    |        |
| 2 |                    |        |
| 3 | JURY INSTRUCTIONS  | 6      |
| 4 |                    |        |
| 5 | GOVERNMENT CLOSING | 38 107 |
| 6 |                    |        |
| 7 | DEFENSE CLOSING    | 73     |
| 8 |                    |        |



9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

4

1 (Thereupon, the following was heard in open  
2 court at 10:03 a.m.)

3 THE COURT: Good morning, everyone.

4 ALL COUNSEL: Good morning, Your Honor.

5 THE COURT: Counsel, I would like to take  
6 up the note from the jury first. Have you all had a  
7 chance to look that over?

8 MS. HAYNES: We have, Your Honor.

9 THE COURT: All right. The government has  
10 a position on it one way or the other?

11 MS. HAYNES: Your Honor, we think that the  
12 juror is qualified to continue to serve.

13 THE COURT: All right.

14 MS. GINSBERG: Your Honor, we agree.

15 THE COURT: Okay. All right. Then the  
16 note will be made a part of the record, and the juror  
17 will be permitted to sit.

18 Counsel, I think that I said at the  
19 beginning of the trial that my plan is at the end of  
20 the -- when the Court's final instruction is given,  
21 before the jury leaves the courtroom, we will select four  
22 names randomly and those jurors will be excluded.

23 I want to address the issue raised by the  
24 defense after our instruction conference on Friday. I'm  
25 happy to hear you now, or have you all agreed to it?

5

1 MS. GINSBERG: Your Honor, I apologize for  
2 the lateness of the instruction, but it wasn't until last  
3 night when I was re-reading the instruction that I think  
4 it's an instruction without the addition is -- leaves a  
5 major omission in what the jury has to find.

6 I think I've seen Your Honor's proposed  
7 addition and change to the verdict form. And I think  
8 that that's adequate. I think that it addresses the  
9 issue.

10 THE COURT: Okay. Let me hear from the  
11 government.

12 MS. HAYNES: Your Honor, we don't object to  
13 the request itself. We would ask that the Court make a  
14 minor modification, the way that this is phrased, we  
15 believe that it should read that with respect to the  
16 information involved in Count I, that it directly  
17 concerned at least one of the following and then continue  
18 on with nuclear weaponry. Because that is, of course,

19 correct that the jury need only find one of the specific  
20 aggravating factors to make this a death penalty eligible  
21 offense.

22 And I think the way it is written, it is  
23 somewhat confusing because it suggests to the jury --

24 THE COURT: That they have to find all of  
25 those.

6

1 MS. HAYNES: Yes.

2 THE COURT: And your suggestion is at least  
3 one.

4 MS. HAYNES: At least one of the following,  
5 colon and then go into the aggravators.

6 MS. GINSBERG: We have no objection. We  
7 think that is a correct statement of the law.

8 THE COURT: Okay. Directly concern at  
9 least one of the following. And that will be in the  
10 verdict form and instruction 29-A -- no, I'm sorry,  
11 instruction 41. Okay. You can bring the jury out.

12 Ladies and gentlemen, by court practices,  
13 once the Court starts instructions, you won't be  
14 permitted to leave the courtroom. The doors will be shut  
15 at least for that period of time that I'm instructing the  
16 jury.

17 (Jury in at 10:07 a.m.)

18 THE COURT: You may be seated. Good  
19 morning, ladies and gentlemen.

20 THE JURORS: Good morning.

21 THE COURT: All right, ladies and  
22 gentlemen, you've now heard all the evidence that's going  
23 to be received in this trial. And you are about to hear

24 the arguments of counsel. And it becomes my duty to give  
25 you the following instructions of the Court as to the law

7

1 as applicable to this case.

2 I'm going to give the instructions to you  
3 orally now and you'll be -- you'll receive a written copy  
4 of the instructions for your consideration during your  
5 deliberations along with the verdict form and all the  
6 evidence that's submitted into the case.

7 It becomes my duty to give you the  
8 following instruction of the Court as to the law that's  
9 applicable to this case. You should use these  
10 instructions to guide you in your decisions.

11 All the instructions of the law given to  
12 you by the judge, those given to you at the beginning of  
13 the trial and those given to you during the trial and  
14 these final instructions, must guide and govern your  
15 deliberations.

16 It is your duty as jurors to follow the law  
17 as stated in all the instructions of the Court and to  
18 apply these rules of law to the facts as you find them to  
19 be from the evidence received during the trial.

20 The attorneys may properly refer to some of  
21 the applicable rules of law in their closing arguments to  
22 you. If, however, any difference appears to you between  
23 the law as stated by the lawyers and that as stated by  
24 the judge in these instructions, you, of course, are to  
25 be governed by the instructions given to you by the

1 judge.

2 You're not to single out any one  
3 instruction alone as stating the law, but must consider  
4 the instructions as a whole in reaching your decisions.  
5 Neither are you to be concerned about the wisdom of any  
6 rule of law stated by the Court.

7 Regardless of any opinion that you may have  
8 as to what the law ought to be, it would be a violation  
9 of your sworn duty to base any part of your verdict upon  
10 any other view or opinion of the law other than given in  
11 these instructions of the Court, just as it would be a  
12 violation of your sworn duty as the judges of the facts  
13 to base your verdict upon anything but the evidence  
14 received in this case.

15 You were chosen as jurors for this trial in  
16 order to evaluate all the evidence received and to decide  
17 each of the factual questions presented by the  
18 allegations brought by the government in the indictment  
19 and in the plea of not guilty by the defendant.

20 In resolving the issues presented to you  
21 for decision in this trial, you must not be persuaded by  
22 bias, prejudice, or sympathy for or against any of the  
23 parties to this case or any public opinion.

24 Justice through trial by jury depends upon  
25 the willingness of each individual juror to seek the

1 truth from the same evidence presented to all the jurors  
2 here in the courtroom and to arrive at a verdict by  
3 applying the same rules of law as now being given to each

of you in these instructions of the Court.

Although the defendant has been indicted, you must remember that an indictment is only an accusation. It is not evidence.

The defendant has pled not guilty to that indictment. As a result of the defendant's pleas of not guilty, the burden is on the prosecution to prove guilt beyond a reasonable doubt.

The burden never shifts to a defendant for the simply reason that the law never imposes upon a defendant in a criminal case the burden or duty of calling any witness or producing any evidence.

The law presumes the defendant to be innocent of all the charges against him. I, therefore, instruct you that the law is to be presumed by you -- the defendant is to be presumed by you to be innocent throughout your deliberations until such time, if ever, you as the jury are satisfied that the government has proven him guilty by proof beyond a reasonable doubt.

The defendant begins the trial here with a clean slate. The presumption of innocence alone is sufficient to acquit a defendant unless you as jurors are

10

unanimously convinced beyond a reasonable doubt of his guilt after careful and impartial consideration of all the evidence in the case.

If the government fails to sustain its burden of proof, you must find the defendant not guilty. This presumption was with the defendant when the trial began and remains with him even now as I speak to you and will continue with the defendant in your

9 deliberations, unless and until you are convinced that  
10 the government has proven his guilt by proof beyond a  
11 reasonable doubt.

12 I've said that the government must prove  
13 the defendant guilty beyond a reasonable doubt. The  
14 question naturally is what is a reasonable doubt? The  
15 words almost define themselves. It is a doubt based upon  
16 reason and common sense. It is a doubt that a reasonable  
17 person has after carefully weighing all the evidence. It  
18 is a doubt which would cause a reasonable person to  
19 hesitate to act in a matter of importance in his or her  
20 personal life.

21 Proof beyond a reasonable doubt must,  
22 therefore, be proof of such a convincing character that  
23 such a reasonable person would not hesitate to rely and  
24 act upon it in the most important of his own affairs.

25 A reasonable doubt is not a caprice or

11

1 whim. It's not speculation or suspicion. It's not an  
2 excuse to avoid the performance of an pleasant duty and  
3 it is not sympathy.

4 In a criminal case, the burden is at all  
5 times upon the government to prove guilt beyond a  
6 reasonable doubt.

7 The law does not require that the  
8 government prove guilt beyond all possible doubt. Proof  
9 beyond a reasonable doubt is sufficient to convict.

10 The burden never shifts to the defendant  
11 which means that it's always the government's burden to  
12 prove each of the elements of the crimes charged beyond a  
13 reasonable doubt.

Regan Trial Feb 10 2003 (Instructions)

14 If after a fair and impartial consideration  
15 of all the evidence you have a reasonable doubt, it is  
16 your duty to acquit the defendant.

17 On the other hand, if after fair and  
18 impartial consideration of all the evidence, you are  
19 satisfied with the defendant's guilt beyond a reasonable  
20 doubt, you should vote to convict.

21 With these preliminary instructions in  
22 mind, let us turn to the charges against the defendant as  
23 contained in the indictment.

24 I remind you that an indictment itself is  
25 not evidence. It merely describes the charges made

12

1 against the defendant. It is an accusation. It may not  
2 be considered by you as evidence -- any evidence of the  
3 guilt of the defendant.

4 In reaching your determination of whether  
5 the government has proved the defendant guilty beyond a  
6 reasonable doubt, you may consider only the evidence  
7 introduced or the lack of evidence.

8 The indictment charges that the offenses  
9 alleged in Counts I and II were committed on or about  
10 certain dates.

11 Although it is necessary for the government  
12 to prove beyond a reasonable doubt that the offenses were  
13 committed on dates reasonably near the dates alleged in  
14 Counts I and II of the indictment, it is not necessary  
15 for the government to prove that the offenses were  
16 committed precisely on the dates charged.

17 The defendant is not on trial for any act  
18 or conduct not specifically charged in the indictment.



19 Count I of the indictment charges that from  
20 in or about January 1999 until on or about August 23,  
21 2001, in the Eastern District of Virginia and elsewhere,  
22 Brian Patrick Regan, with the intent and reason to  
23 believe that they were to be used to the injury of the  
24 United States and to the advantage of a foreign  
25 government, specifically Iraq, did knowingly and unlawful

13

1 attempt to communicate, deliver and transmit to a foreign  
2 government, specifically Iraq and to representatives,  
3 officers, agents and employees thereof, directly and  
4 indirectly, documents and information relating to the  
5 national defense of the United States, which documents  
6 and information were classified top secret, SCI and which  
7 directly concerned satellites, early warning systems,  
8 means of defense or retaliation against large scale  
9 attack, communications intelligence information, and  
10 major elements of defense strategy.

11 Count II of the indictment charges that  
12 from at least in or about January, 1999, until on or  
13 about August 23, 2001, in the Eastern District of  
14 Virginia and elsewhere, Brian Patrick Regan, with the  
15 intent and reason to believe that they were to be used to  
16 the injury of the United States and to the advantage of a  
17 foreign government, specifically Libya, did knowingly and  
18 unlawful attempt to communicate, deliver and transmit to  
19 a foreign government, specifically Libya, and to  
20 representatives, officers, agents and employees thereof,  
21 directly and indirectly documents and information  
22 relating to the national defense of the United States,  
23 which documents and information were classified top

24 secret, SCI and which directly concerned satellites,  
25 early warning systems, means of defense or retaliation

14

1 against large scale attack, communications intelligence  
2 information and major elements of defense strategy.  
3 Count III of the indictment charges that  
4 from at least in or about January, 1999, until on or  
5 about August 23, 2001, in the Eastern District of  
6 Virginia and elsewhere, Brian Patrick Regan, with the  
7 intent and reason to believe that they were to be used to  
8 the injury of the United States and to the advantage of a  
9 foreign government, specifically the People's Republic of  
10 China, did knowingly and unlawful attempt to communicate,  
11 deliver and transmit to a foreign government,  
12 specifically the People's Republic of China and to  
13 representatives, officers, agents, and employees thereof,  
14 directly and indirectly, documents and information  
15 relating to the national defense of the United States.

16 Counts I, II, and III each charge the  
17 defendant, Brian Patrick Regan, with attempted espionage.

18 The crime of attempted espionage in  
19 violation of Section 9 -- 794(A) of Title 18 of the  
20 United States Criminal Code reads in pertinent part as  
21 follows: whoever with the intent or reason to believe  
22 that it is to be used to the injury of the United States  
23 or to the advantage of a foreign nation communicates,  
24 delivers or transmits or attempts to communicate, deliver  
25 or transmit to any foreign government or to any faction

or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject or citizen thereof, either directly or indirectly any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance or information relating to the national defense shall be guilty of an offense against the United States.

The essential elements of attempted espionage, each of which the government must prove beyond a reasonable doubt, are as follows. First, that the defendant attempted to communicate, deliver or transmit documents or information relating to the national defense to a foreign government or to representatives, officers, agents and employees thereof.

Second, that the defendant acted with the intent or reason to believe that the documents or information in question were to be used to the injury of the United States or to the advantage of a foreign nation.

And third, that the defendant acted willfully.

In addition, if the jury concludes that the defendant is guilty of Count I or Count II with respect

to each count, the jury must specify in the verdict form whether it finds beyond a reasonable doubt that the documents and information directly concerned at least one

4 of the following, nuclear weaponry, military satellites,  
5 early warning systems, other means of defense or  
6 retaliation against large scale attack, war plans,  
7 communications intelligence, or cryptographic information  
8 or any other major weapon system or major element of  
9 defense strategy.

10 In order to prove the charge of attempting  
11 to commit the crime charged, it is necessary that the  
12 evidence establish beyond a reasonable doubt, one, that  
13 the defendant intended to commit the crime charged, and  
14 two, that the defendant willfully took some action that  
15 was a substantial step in an effort to bring about or to  
16 accomplish the crime which is strongly corroborative of  
17 that intent.

18 Mere intention to commit a specific crime  
19 does not amount to an attempt. In order to convict the  
20 defendant of an attempt, you must find beyond a  
21 reasonable doubt that the defendant intended to commit  
22 the crime charged and that he took some action which was  
23 a substantial step toward the commission of that crime.

24 In determining whether the defendant's  
25 actions amounted to a substantial step toward commission

17

1 of that crime, it is necessary to distinguish between  
2 mere preparation on the one hand and the actual doing of  
3 the criminal deed on the other.

4 Mere preparation which may consist of  
5 planning the offense or of devising, obtaining or  
6 arranging the means for its commission is not an attempt,  
7 although some preparations may amount to an attempt.

8 The acts of a person who intends to commit  
Page 14

9 a crime will constitute an attempt where the acts  
10 themselves clearly indicate an intent to willfully commit  
11 the crime and the acts are a substantial step in a course  
12 of conduct planned to culminate in the commission of the  
13 crime.

14 Count IV of the indictment charges that  
15 from at least in or about January, 1999, through on or  
16 about August 23, 2001, in the Eastern District of  
17 Virginia and elsewhere, the defendant Brian Patrick Regan  
18 did, for the purpose of obtaining information respecting  
19 the national defense, with intent and reason to believe  
20 that the information was to be used to the injury of the  
21 United States and to the advantage of a foreign nation,  
22 did unlawfully and knowingly copy, take, make and obtain  
23 classified secret and top secret photographs, plans,  
24 maps, documents, writings and notes connected with the  
25 national defense.

18

1 Count IV charges Brian Patrick Regan with  
2 gathering national defense information. Section 793(B)  
3 of Title 18 of the United States Criminal Code reads as  
4 follows: whoever, for the purpose of obtaining  
5 information respecting the national defense with intent  
6 or reason to believe that the information is to be used  
7 to the injury of the United States or to the advantage of  
8 any foreign nation, copies, takes, makes or obtains or  
9 attempts to copy, take, make or obtain any sketch,  
10 photograph, photographic negative, blueprint, plan, map,  
11 model, instrument, appliance, document, writing, or note  
12 of anything connected with national defense, shall be  
13 guilty of an offense against the United States.

14           This count charges the defendant with  
15 illegally gathering or obtaining of information relating  
16 to the national defense.

17           The essential elements of the offense, each  
18 of which the government must prove beyond a reasonable  
19 doubt, are as follows. First, that the defendant did  
20 take -- that the defendant did copy, take, make, or  
21 obtain any document.

22           Second, that the defendant copied, took,  
23 made or obtained the document or documents for the  
24 purpose of obtaining information related to the national  
25 defense and with the intent or reason to believe that the

19

1 information was to be used to the injury of the United  
2 States or to the advantage of any foreign nation.

3           And, third, that the defendant acted  
4 willfully.

5           The definitions I've previously provided to  
6 you with respect to national defense, the intent or  
7 reason to believe that information is to be used to the  
8 injury of the United States or to the advantage of a  
9 foreign nation, foreign -- or willfully apply to this  
10 count as well.

11           You've been instructed that in order to  
12 sustain its burden of proof, the government must prove  
13 the defendant acted willfully.

14           willfully means to act with knowledge that  
15 one's conduct is unlawful and with the intent to do  
16 something the law forbids, that is to say, with bad  
17 purpose to disobey or to disregard the law.

18           The defendant's conduct was not willful if

19 it was due to negligence, inadvertence or mistake.  
20 You've been instructed that in order to  
21 sustain its burden of proof, the government must prove  
22 that the defendant acted knowingly. A person acts  
23 knowingly if he acts intentionally and voluntarily and  
24 not because of ignorance, mistake, accident or  
25 carelessness.

20

1 whether the defendant acted knowingly may  
2 be proven by the defendant's conduct and by all of the  
3 facts and circumstances surrounding the case.

4 Proof of motive is not a necessary element  
5 of the crimes with which the defendant is charged. Proof  
6 of motive does not establish guilt nor does want of proof  
7 of motive establish that a defendant is innocent.

8 If the guilt of the defendant is shown  
9 beyond a reasonable doubt, it is immaterial what the  
10 motive for the crime may be or whether any motive was  
11 shown. But the presence or absence of motive is a  
12 circumstance which you may consider as bearing on the  
13 intent of a defendant.

14 For purposes of the charge in the  
15 indictment, the term foreign refers to any country other  
16 than the United States, regardless of whether the country  
17 is an ally or enemy of the United States.

18 With intent, with respect to an  
19 espionage-related charge, means that the defendant acted  
20 in bad faith and with a deliberate purpose to disregard  
21 or disobey the law.

22 Reason to believe with respect to an  
23 espionage-related charge means that the defendant knew

24 facts from which he concluded or reasonably should have  
25 concluded that the document, writings, photographs, or

21

1 information relating to the national defense would be  
2 used for the prohibited purposes.

3 In considering whether or not the defendant  
4 acted with the intent or having reason to believe that  
5 the material would be used to the injury of the United  
6 States or to the advantage of a foreign country, you may  
7 consider the nature of the documents or information  
8 involved.

9 The government does not have to prove that  
10 the documents or information could be used both to injure  
11 the United States and to the advantage of a foreign  
12 country. The statute reads in the alternative. So,  
13 proof of either will suffice.

14 Further, the country to whose advantage the  
15 information would be used need not necessarily be an  
16 enemy of the United States. The statute does not  
17 distinguish between friend and enemy.

18 The term national defense is a broad term  
19 which refers to the United States military and naval  
20 establishments and to all related activities of national  
21 preparedness.

22 To prove that the documents, writings,  
23 photographs or information relate to the national  
24 defense, there are two things that the government must  
25 prove.



1 First, they must prove that the disclosure  
2 of the material would be potentially damaging to the  
3 United States or might be useful to an enemy of the  
4 United States.

5 Second, it must prove that the material is  
6 closely held by the United States government. Where the  
7 information has been made public by the United States  
8 government and is found in sources lawfully available to  
9 the general public, it does not relate to national  
10 defense.

11 Similarly, where the sources of information  
12 are lawfully available to the public and the United  
13 States government has made no efforts to guard such  
14 information, the information, itself, does not relate to  
15 the national defense.

16 In determining whether a material is  
17 closely held, you may consider whether it has been  
18 classified by appropriate authorities and whether it  
19 remained classified on the date or dates pertinent to the  
20 indictment.

21 You've heard about both the classification  
22 of information at issue in this case and the possibility  
23 that some of the information may be publicly available.

24 You may consider whether the information  
25 was classified or not in determining whether the

1 information relates to the national defense.

2 However, the fact that the information is  
3 designated as classified does not, in and of itself,  
Page 19

demonstrate that the information relates to the national defense.

The government bears the burden of proving beyond a reasonable doubt that the information relates to the national defense.

137

CERTIFICATE OF REPORTER

I, Renecia Wilson, an official court reporter for the United State District Court of Virginia, Alexandria Division, do hereby certify that I reported by machine shorthand, in my official capacity, the proceedings had upon the trial in the case of United States of America vs. Brian Patrick Regan.

I further certify that I was authorized and did report by stenotype the proceedings and evidence in said trial, and that the foregoing pages, numbered 1 to 136, inclusive, constitute the official transcript of said proceedings as taken from my shorthand notes.

IN WITNESS WHEREOF, I have hereto subscribed my name this       day of       , 2003.

Renecia Wilson, RMR/CM  
Official Court Reporter



UNITED STATES OF AMERICA )

v. )

Manning, Bradley E. )  
PFC, U.S. Army, )  
HHC, U.S. Army Garrison, )  
Joint Base Myer-Henderson Hall )  
Fort Myer, Virginia 22211 )

Prosecution Motion

for Preliminary Ruling on  
Admissibility of Evidence  
(Business Records)

22 June 2012

RELIEF SOUGHT

The prosecution in the above case respectfully requests that this Court admit into evidence the following authenticated business records in advance of trial: the Accused's Official Military Personnel File (OMPF) from Human Resources Command (HRC); the Accused's unit Soldier Management Individual File (SMIF); the United States Office of Personnel Management (OPM) investigation and supporting documents for the Accused; Army Training Requirement and Resources System (ATRRS) records; 35F10 AIT Program of Instruction (POI), lesson plans, and Student Evaluation Plan; the Department of Defense (DoD) IA Information Assurance (IA) version 7 (dated October 2008) and version 8 (dated October 2009); IA screenshot; IAVTC screenshot; Joint Asset Movement Management System (JAMMS) records for the Accused; Sensitive Compartmented Information (SCI) Packet for the Accused; and a Distributed Common Ground System-Army (DCGS-A) Certificate of Networthiness (CON) list. The prosecution seeks said relief to provide improved predictability and efficiency to the proceedings.

This motion also serves as notice to the defense that the government intends on offering these documents as evidence under Military Rule of Evidence (MRE) 902(11).

BURDEN OF PERSUASION AND BURDEN OF PROOF

The burden of proof on any factual issue, the resolution of which is necessary to decide a motion, shall be by preponderance of the evidence. RCM 905(c)(1). The burden of persuasion on any factual issue, the resolution of which is necessary to decide a motion, shall be on the moving party. RCM 905(c)(2). The prosecution has the burden of persuasion as the moving party.

FACTS

On 26 September 2007, the Accused enlisted in the Army as an E-1 for four (4) years Active Duty and four (4) years Reserve time. His commitment began on 2 October 2007 and his Military Occupational Specialty (MOS) was a 35F Intelligence Analyst. A copy of his Enlistment/Reenlistment Document is maintained in his OMPF. See Enclosure 1.

On 26 September 2007, the Accused completed a Security Clearance Application, a copy of which is maintained in the Accused's local unit file. See Enclosure 2. There was missing information noted on the form. On 2 October 2007, the Accused completed another Security Clearance Application, a copy of which is maintained in his OMPF. See Enclosure 1.

On 2 October 2007, the Accused received orders to report to Fort Leonard Wood, Missouri on 2 October 2007. A copy of the orders is maintained in the Accused's local unit file. See Enclosure 2.

On 15 January 2008, OPM closed their background investigation on the Accused. See Enclosure 3.

The Accused signed a Classified Information Nondisclosure Agreement (NDA) on 7 April 2008, while at Fort Huachuca, Arizona. A copy of the NDA is maintained in his OMPF. See Enclosure 1.

From 11 April 2008 to 14 August 2008, the Accused attended 35F Advanced Individual Training (AIT). See Enclosure 4. At AIT, the Accused was taught how to be an intelligence analyst for the Army. Training at AIT included how to properly mark and handle classified information, the meaning of the various classifications, how to effectively use the internet, the value of the internet in research and collection, and operational security and the enemy's use of the internet. See Enclosures 5 and 6.

On 14 August 2008, the Accused left AIT at Fort Huachuca and, on 27 August 2008, reported to his first unit (2-10 Mountain, Fort Drum, New York). His MOS was 35F. A copy of his orders and pass form are maintained in the Accused's individual unit file. The Accused was assigned to this unit and deployed to Iraq when the charged misconduct occurred. See Enclosure 2.

On 5 September 2008, the Accused completed his required annual IA training. The training is administered by the IA Branch and requires the individual to pass a test. See Enclosures 7, 8 and 10.

On 17 September 2008, the Accused signed another Classified Information NDA. See Enclosure 14.

On 21 January 2009, the Accused was nominated by his Brigade Security Manager for SCI Access. The Accused signed a SCI Pre-Indoctrination Screening Interview form on 22 January 2008 and answered "no" to all of the questions asked. The Accused also signed an SCI Security Awareness and Defense Travel Briefing, a Pre-Nondisclosure Execution Briefing, a Personal Attestation upon the Granting of Security Access, an SCI NDA, an addendum to the NDA, and an acknowledgment of Special Access Program briefings on 22 January 2009. On 28 January 2009, the Accused signed another SCI NDA. See Enclosure 14.

Movement reports are maintained on Soldiers on a system called JAMMS as they enter and leave theater. On 12 October 2009, the Accused arrived in Kuwait, and on 28 October 2009, the Accused arrived in Iraq. See Enclosure 11.

On 31 October 2009, the Accused completed his required annual IA training. The training is administered by the IA Branch and requires the individual to pass a test. See Enclosures 8 and 10.

On 22 January 2010, the Accused left Iraq on Environmental Morale Leave (EML); on 11 February 2010, the Accused arrived back in Iraq; and on 14 February 2010, the Accused arrived back at FOB Hammer. See Enclosure 11. The Government has alleged misconduct that occurred prior to the Accused leaving Iraq on EML, misconduct that occurred while the Accused was in the United States, and misconduct that occurred beginning almost immediately after the Accused arrived back in Iraq. See Charge Sheet.

While in Iraq, the Accused was an intelligence analyst and worked on the DCGS-A system. See Enclosure 12. The DCGS-A system is a type of computer workstation used by intelligence analysts that is connected to the Secret Internet Protocol Router Network (SIPRNET). See Enclosure 13. The DCGS-A CON List is a list of what software can be loaded on the DCGS-A computer. The list also refers to AR 25-2. See Enclosure 15.

On 22 April 2010, the Accused began the 2010 annual U.S. Army Information Assurance Virtual Training Classroom (IAVTC) that Soldiers and Department of the Army employees utilize to complete non-mandatory IA training. See Enclosures 9 and 10.

On 24 May 2010, the Accused received an Article 15 for punching SPC Jihreah Showman in the face with a closed fist on 8 May 2010. A copy of the Article 15 is maintained in the Accused's local unit file. See Enclosure 2. Because of this misconduct, the Accused was removed from the 2-10 Mountain Sensitive Compartmented Information Facility (SCIF) and assigned to work in the supply room. The prosecution has charged the Accused with stealing or converting the United States Forces-Iraq (USF-I) Global Address List (GAL) after he was removed from the SCIF. See Charge Sheet.

On 29 May 2010, the Accused was ordered into confinement by his company commander, CPT Freeburg. A copy of the Confinement Order and supporting documentation is maintained in the Accused's local unit file. See Enclosure 2.

On 30 May 2010, the Accused left Iraq. See Enclosure 11.

On 3 February 2012, the following charges were referred against the Accused: one specification of violating Article 104, aiding the enemy; one specification of violating Article 134, for wrongfully and wantonly causing to be published on the internet intelligence belonging to the United States government, having knowledge that intelligence published on the internet is accessible to the enemy; eight specifications of violating Article 134 for willfully communicating or transmitting national defense information to a person not entitled to receive it, in violation of 18 USC § 793(e); two specifications of violating Article 134 for exceeding authorized access on a SIPRNET computer, in violation of 18 USC § 1030(a)(1); five specifications of violating Article 134 for stealing or converting Government property, in violation of 18 USC § 641; and five specifications alleging misconduct in violation of Article 92, including specifications alleging that the accused violated Army Regulation 25-2 by adding unauthorized software to a SIPRNET

computer and using an information system in a manner other than its intended purpose. See Charge Sheet.

### WITNESSES/EVIDENCE

The prosecution requests you consider the following:

- Charge Sheet
- Listed Enclosures

### LEGAL AUTHORITY AND ARGUMENT

The trial judge has discretion as to the manner in which she makes preliminary determinations concerning the admissibility of evidence. MRE 104; see U.S. v. Blanchard, 48 M.J. 306 (C.A.A.F. 1998). This judicial discretion includes "preadmitting" evidence provided it is relevant and no other rule prohibits its admission. See, e.g., U.S. v. Bradford, 68 M.J. 371 (C.A.A.F. 2010). Where, as here, there is no question as to the admissibility of the evidence, the enclosed records should be preadmitted to provide predictability to both parties and to dispose of what amounts to administrative matters outside the presence of the panel (assuming there is a panel).

#### I. THE RECORDS ARE RELEVANT.

Evidence that has a tendency to make a fact of consequence more or less probable than it would be without the evidence is relevant. MRE 401. All relevant evidence is generally admissible. MRE 402.

##### A. OMPF

The Accused's OMPF records are relevant on their face to all charges and specifications. The personnel records create the complete picture of the Accused's time as a Soldier. Specifically, his Enlistment/Reenlistment Document shows how long he has been in the military and is relevant to his training and experience as a Soldier. The Accused's completion of the 2 October 2007 Security Clearance Application, at least a second one, shows his familiarity with the process as well as the seriousness and importance of not omitting information required to complete the form and the background check. The NDA signed by the Accused on 7 April 2008, while at Fort Huachuca, Arizona, is evidence of his knowledge of what can and cannot be disclosed to the public and his familiarity with several of the charged offenses which are spelled out in the NDA.

The file is also generally relevant to provide a complete picture of the Accused's career, including a timeline of relevant training and education events for the trier of fact, and the above information is specifically relevant to the scienter required for the Accused to have knowingly committed the offenses.

##### B. SMIF

The Accused's SMIF records are relevant on their face to all charges and specifications. The personnel records create the complete picture of the Accused's time as a Soldier. Specifically,

the Accused's completion of the 26 September 2007 Security Clearance Application shows his introduction to the security clearance process and its rules and regulations. The Accused's orders to basic training on 2 October 2007 show his entry into the military and the beginning of a litany of training. The Accused's subsequent orders show that he went to Fort Huachuca, Arizona for AIT and left on 14 August 2008 to report to his unit, 2-10 Mountain, Fort Drum, New York on 27 August 2008. His MOS was 35F; therefore, he was a trained intelligence analyst. The Article 15 precipitated the Accused being removed from the SCIF and reassigned to the supply room where he continued his misconduct by stealing the USF-I GAL. See Charge Sheet. Finally, the 29 May 2010 confinement order and supporting documentation show when the Accused was discovered and the misconduct ended.

The file is generally relevant to show a timeline of the Accused's career. The Accused's training and security clearance application are specifically relevant to the scienter required for the Accused to have knowingly committed the offenses. The Article 15 also reveals why the Accused was removed from the SCIF and sent to work in the supply room and provides a timeline which corresponds to misconduct committed from computers in the supply room. The confinement order shows a timeline of the Accused's access to information and why the information harvesting stopped on approximately 29 May 2010.

#### C. OPM Investigation and Supporting Documents

The OPM information is relevant to all charges and specifications. It shows that the Accused went through the entire security clearance process and the U.S. Government determined, based on his answers, that he was worthy of the special trust instilled in someone who is granted a security clearance.

#### D. ATRRS

The ATRRS records are relevant on their face to all charges and specifications. They establish when the Accused attended AIT at Fort Huachuca. The ATRRS records also list the course title ("intelligence analyst") for the training attended at Fort Huachuca. In short, the training records provide more information on the timeline of the Accused's career and prove that the Accused attended and completed training relevant to the charges and specifications in this case.

#### E. AIT Records (POI, Lesson Plans, and SEP)

The Accused's AIT records are relevant on their face to all charges and specifications. They show when and how the Accused was trained. Specifically, the program of instruction for course 243-35F10, Version 1 shows the training that 35F AIT Soldiers received, including the course lesson plan, the content of the lectures and the PowerPoints, the length of time each lecture should take, the learning objectives, and the evaluations or assignments given to Soldiers. The program of instruction reveals that during AIT, students were instructed on how to properly mark and handle classified information, the meaning of the various classifications, how to effectively use the internet, the value of the internet in research and collection, and operational security and the enemy's use of the internet. Specifically, Slide 73 of the Powerpoint presentation, entitled



Prevent Disclosure, asks and responds to the following, "Would you give this information to a terrorist? If the answer is "no," DON'T PUT IT ON THE WEB!!!" The student evaluation plan shows the lesson plans, the instruction, and performance objectives, as well as the requirements for the course examinations.

The file is generally relevant to show a timeline of the Accused's AIT training and is particularly relevant as proof that the Accused knowingly committed the offenses.

#### F. DoD IA Awareness Training

The IA certifications and training are relevant to all charges and specifications. The training teaches Soldiers and DA civilians the importance of maintaining the integrity of the Army systems. The 5 September 2008 and 31 October 2009 training confirmations reveal that the Accused did receive the required training, and the IAVTC screenshot confirms that the Accused at least started additional non-required training on 22 April 2010. IA training was yet another opportunity the U.S. Army took to train the Accused on proper handling of information and the proper use of information systems, and again, provides evidence that the Accused had knowledge of information assurance principles. In short, all of the alleged misconduct in this case is related in some way to the Accused's use of computers or information systems. See Charge Sheet.

#### G. JAMMS Movement Report

The Accused's JAMMS Movement Report is relevant because it shows when the Accused arrived in Iraq for his deployment, when the Accused was on EML from Iraq, when the Accused returned from EML, and when the Accused left Iraq. The JAMMS report is a definitive timeline of the Accused's travel that provides compelling evidence of the Accused's location during time periods relevant to the charges. See Charge Sheet.

#### H. SCI Indoctrination Packet

The Indoctrination Packet is relevant to the charges relating to the compromise of classified information. The Indoctrination Packet shows that beginning on 17 September 2008, the Accused again was informed of the importance of protecting classified information and in particular was told that unauthorized disclosure of classified information may constitute a violation of 18 U.S.C. §§ 641 and 793(e). On 21 January 2009, the Accused was nominated by his Brigade Security Manager for SCI Access. After that, the Accused signed numerous forms which asked additional background questions and ensured that the signatory was aware of the importance of protecting classified information and the criminal liabilities involved in disclosing that information to unauthorized individuals. See Enclosure 14. Through eleven different signatures and sixteen different initials, the SCI Packet and supporting documentation show the Accused received extensive information and knew the extent of his misconduct when he compromised the charged classified information. See Charge Sheet.

#### I. DCGS-A CON List

The DCGS-A CON list is relevant to the Article 92 violations alleging that the Accused added unauthorized software to a SIPRNET computer. Specifically, the United States must prove that Wget was unauthorized software when the Accused added it to his work computers on the dates specified on the Charge Sheet. The DCGS-A CON list is proof that Wget was not certified as "networthy" by the Army.

## II. THE RECORDS ARE NOT EXCLUDABLE AS HEARSAY BECAUSE THEY ARE RECORDS OF REGULARLY CONDUCTED ACTIVITY.

Hearsay is an out-of-court statement, written or oral, offered for the truth of the matter asserted. MRE 801(c). Hearsay is often excluded as evidence during trial due to doubts of the evidence's reliability. The general prohibition of hearsay evidence has several exceptions, including an exception under MRE 803(6) for "records of regularly conducted activity" as they are inferentially reliable. See MRE 803(6). "Records of regularly conducted activity" is defined as the following:

[a] memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Mil. R. Evid. 902(11) or any other statute permitting certification in a criminal proceeding in a court of the United States, unless the source of the information or the method or circumstances or preparation lack trustworthiness.

MRE 803(6).

Several of the records are specifically cited in the rule as being examples of information normally admissible as a record of regularly conducted activity, such as enlistment papers, service records, and unit personnel diaries. MRE 803(6). All enclosed records are records of regularly conducted activity, and there is no evidence that any of the records lack trustworthiness. All enclosed records are, therefore, admissible under MRE 803(6) as exceptions to hearsay. In addition, all enclosed records are accompanied by attestations made in accordance with MRE 902(11), authenticating them as business records.

## III. THE RECORDS ARE AUTHENTIC.

In addition to being relevant, evidence must also be authentic to be admissible. See MRE 901(a). "[A]dmissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." MRE 901(a). Some evidence, however, is self-authenticating and does not require "[e]xtrinsic evidence of authenticity as a condition precedent to admissibility." MRE 902. "Certified domestic records of regularly conducted activity" fall

under this exception. MRE 902(11). Pursuant to MRE 902(11), extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to certified domestic records of a regularly conducted activity when:

[t]he original or a duplicate of a document or record of regularly conducted activity that would be admissible under Mil R. Evid. 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority certifying that the record (A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters; (B) was kept in the course of the regularly conducted activity; and (C) was made by the regularly conducted activity as a regular practice.

MRE 902(11).

The following attestations were made in accordance with MRE 902(11):

On 18 April 2012, Mr. Domingo U. Contu, HR Assistant, iPerms Support Team, Army Soldier Records Branch, U.S. Army Human Resources Command, as custodian of Soldier OMPF records, certified all documents filed in the Accused's OMPF.

On 24 April 2011, CPT Matthew W. Freeburg, as Company Commander of HHC, 2d Brigade Combat Team, 10th Mountain Division (Light), Fort Drum, NY, attested to the authenticity of the unit Soldier Management Individual File (SMIF) of the Accused (144 pages).

On 17 April 2012, Ms. Lisa Alleman, Supervisory FOI/PA Specialist, attested to the authenticity of the Single Scope Background Investigation and Entrance National Agency Check Investigation on the Accused.

On 11 June 2012, Mr. Ralph Steinway, Chief, Training Division, Headquarters, DA G-1, attested to the authenticity of ATRRS records, specifically the "Student Portal Reservation by Student Function (Training History All) Manning, Bradley ( )" and "IET Trainee Processing, Manning, Bradley ( )."

On 13 July 2011, Ms. Theresa Robinson, Management Analyst, Defense Information System Agency (DISA), attested to the authenticity of the DoD IA Awareness version 7 (dated October 2008) and the DoD IA Awareness version 8 (dated October 2009).

On 31 January 2012, Mr. Doug Schastecn, IT Director, Willco Technologies, Inc., as custodian of Army Training and Certification Tracking System, attested to the authenticity of the Accused's Army training and certification screenshots.

On 27 January 2012, Mr. Ryan Fidler, Director of Development, attested to the authenticity of an IA Virtual Training screenshot entitled "IA Virtual Training.pdf (1 Page)."

On 15 February 2012, Ms. Mary Amiatu, SAMD Clerk, US ARCENT G1 SAMD Section, attested to the authenticity of the JAMMS records pertaining to the Accused as of 15 February 2012.

On 13 February 2012, CW3 Anthony L. Barnett, 35F10 Committee Chief, attested to the authenticity of the program of instruction and lesson plan for the Intelligence Analyst Course, specifically a DVD-R containing two RTF Files named "243-35F10 Ver1 POI.RTF" and "243-35F10 Ver1 Lesson Plans.rtf."

On 6 February 2012, CW3 Anthony L. Barnett, 35F10 Committee Chief, attested to the authenticity of the student evaluation plan for the 35F10 Intelligence Analyst Course, specifically the "35F10 Student Evaluation Plan (SEP)."

On 8 February 2012, Ms. Tina Huffman, SCI Program Manager, attested to the authenticity of all documents filed in the Accused's SCI Indoctrination packet, specifically "INDOC - COMINT - 29 Jan 10.pdf (1 Page)"; "JCAVS Report - 26 May 2010.pdf (2 pages)"; and "SCI Packet - Jan 2009.pdf (22 pages)."

On 11 April 2012, Ms. Florinda White, Program Manager, DCGS-A Configuration Management, attested to the authenticity of the Version Description Document (VDD) for the Basic Analyst Laptop (BAL), Distributed Common Ground Systems-Army, Software Version 3.1 Patch 3 (DCGS-A V3.1 P3), dated 1 October 2009, title "DCGS-A\_V3.1\_P3\_BAL\_VDD\_149015\_Rev1\_1\_Oct\_09.doc (14 pages)."

Written declarations made in accordance with MRE 902(11) accompany all the enclosed files; therefore, all the records are properly authenticated.

#### IV. THE DUPLICATE RECORDS ARE ADMISSIBLE TO THE SAME EXTENT AS AN ORIGINAL

"A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original, or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original." MRE 1003. A duplicate is defined as "a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic rerecording, or by chemical reproduction, or by other equivalent techniques which accurately reproduce the original. MRE 1001(4). The contents of an official record, . . . including data compilations in any form, if otherwise admissible, may be proved by copy, certified as correct or attested to in accordance with Mil. R. Evid. 902 or testified to be correct by a witness who has compared it with the original. If a copy which complies with the foregoing cannot be obtained by the exercise of reasonable diligence, then other evidence of the contents may be given. MRE 1005.

In the certifications for all of the enclosed records, the records custodian specifically states that the records are true and accurate or complete copies of the originals. There is no evidence that any of the original documentation may not be authentic, nor is there any circumstance present which would make the admission of a duplicate in lieu of the original unfair. The enclosures include official records, and all of them are business records. The duplicates, therefore, are admissible to the same extent as the originals.

V. THE PROBATIVE VALUE OF THE RECORDS IS NOT SUBSTANTIALLY OUTWEIGHED BY UNFAIR PREJUDICE.

Courts may exclude relevant evidence if its probative value is substantially outweighed by the danger of unfair prejudice, confusion, or waste of time. MRE 403. Prejudice alone is not sufficient to warrant exclusion. Virtually all evidence is prejudicial to one party or another. To justify exclusion the prejudice must be unfair. United States v. Candelaria-Silva, 162 F.3d 698, 705 (1st Cir. 1998).

As stated in Section I, all the evidence is relevant to the charged offenses. The OMPF, the SMIF, and JAMMS report establish a timeline of the Accused's career and when he was present in Iraq. His security clearance information shows that he applied for and was granted clearance based on his representations. The OMPF, SCI Packet, DoD IA Training, ATRRS, and AIT Records all show how extensively the Accused was trained on Information Assurance, INFOSEC, and OPSEC. The DCGS-A CON list shows that the Accused installed software on his computer that he was not allowed to install in violation of AR 25-2. The knowledge instilled by these various training tools establishes that the Accused knew what he was doing was wrong and that if transmitted information to Wikileaks, it would end up in the hands of the enemy.

The evidence is prejudicial to the Accused in that it builds the case against him and shows his awareness of what he was doing; however, it is not unfairly prejudicial. All of the records are relevant to the Accused and the charged offenses and are a direct result of the Accused's actions. The records help establish a timeline to make the events clear to the factfinder and they assist in proving the scienter required for the offenses.

CONCLUSION

Based upon the requirements for admissibility of evidence in accordance with MRE 104, MRE 401, MRE 402, MRE 403, MRE 803(6), and MRE 902(11), the Government respectfully moves this court, pursuant to RCM 906(13), to pre-admit the Accused's OMPF from HRC; the Accused's SMIF; JAMMS records; SCI Packet; DoD IA Awareness version 7 (dated October 2008); DoD IA Awareness version 8 (dated October 2009); Army Training and Certification screenshot; 243-35F10 Ver 1 POI RTF; 243-35F10 Ver 1 lesson plans; 35F10 Student Evaluation Plan as they are on their face relevant to the charges at issue and will provide improved predictability and efficiency to the proceedings.



ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on Defense Counsel via electronic mail, on 22 June 2012.



ANGEL M. OVERGAARD  
CPT, JA  
Assistant Trial Counsel

15 Enclosures

1. Accused's OMPF from HRC w/ attestation
2. Accused's SMIF w/ attestation
3. OPM Investigation and Supporting Documents w/ attestation
4. ATRRS records w/ attestation
5. 35F10 AIT POI and Lesson Plan w/ attestation
6. 35F10 AIT Student Evaluation Plan w/ attestation
7. DoD IA Awareness version 7 (dated October 2008) and version 8 (dated October 2009) w/ attestation
8. IA Screenshot w/ attestation
9. IAVTC Screenshot w/ attestation
10. AIR, SA Bettencourt, dated 21 Jan 11
11. JAMMS records w/ attestation
12. AIR, SA Kim, dated 31 Aug 10
13. DCGS-A Information Sheet
14. SCI Packet w/ attestation
15. DCGS-A CON List w/attestation

UNITED STATES OF AMERICA

v.

Manning, Bradley E.  
PFC, U.S. Army,  
HHC, U.S. Army Garrison,  
Joint Base Myer-Henderson Hall  
Fort Myer, Virginia 22211

Prosecution Motion

for Preliminary Ruling on  
Admissibility of Evidence  
(Business Records)

Enclosure 1

22 June 2012



DEPARTMENT OF THE ARMY  
U.S. ARMY HUMAN RESOURCES COMMAND  
1600 SPEARHEAD DIVISION AVENUE  
FORT KNOX, KY 40122

AHRC-PDR-R

April 18, 2012

MEMORANDUM FOR Headquarters, Fort Lesley J. McNair, DC 20319

SUBJECT: Certification of Official Military Personnel File (OMPF) pertaining to:  
PFC Manning, Bradley E. [REDACTED]

1. Per your request, and under the provisions of AR 600-8-104, paragraph 2-3, the attached documents are released. I certify that the released OMPF of the Soldier named is a true and complete copy of the OMPF maintained at this record site. In witness whereof, I have this date hereunto set by hand and affixed the seal of the Army Human Resources Command-Fort Knox, Department of the Army, 1600 Spearhead Division Avenue, Fort Knox, Kentucky 40122-5000.
2. This memorandum certifies that Soldier OMPFs are maintained by the Army Soldier Records Branch within the Army Human Resources Command-Fort Knox, as required by appropriate regulations. As custodian of these records, the undersigned is authorized to certify official records, reports, entries, or documents filed therein.
3. Point of contact is the undersigned at COMM 502-613-9990, DSN 983-613-9990.

End

*Domingo U. Condu*  
Domingo U. Condu  
HR Assistant, IP/HRMS Support Team  
Army Soldier Records Branch





NAME: MANNING, BRADLEY EDWARD SSN: [REDACTED]

## RECORD OF EMERGENCY DATA

## PRIVACY ACT STATEMENT

AUTHORITY: 5 USC 552, 10 USC 655, 1475 to 1480 and 2771, 38 USC 1970, 44 USC 3101, and EO 9397 (SSN).

PRINCIPAL PURPOSES: This form is used by military personnel and Department of Defense civilian and contractor personnel, collectively referred to as civilians, when applicable. For military personnel, it is used to designate beneficiaries for certain benefits in the event of the Service member's death. It is also a guide for disposition of that member's pay and allowances if captured, missing or interned. It also shows names and addresses of the person(s) the Service member desires to be notified in case of emergency or death. For civilian personnel, it is used to expedite the notification process in the event of an emergency and/or death of the member. The purpose of soliciting the SSN is to provide positive identification. All items may not be applicable.

ROUTINE USES: None.

DISCLOSURE: Voluntary; however, failure to provide accurate personal identifier information and other solicited information will delay notification and the processing of benefits to designated beneficiaries if applicable.

## INSTRUCTIONS TO SERVICE MEMBER

This extremely important form is to be used by you to show the names and addresses of your spouse, children, parents, and any other person(s) you would like notified if you become a casualty (other family members or fiancé), and, to designate beneficiaries for certain benefits if you die. IT IS YOUR RESPONSIBILITY to keep your Record of Emergency Data up to date to show your desires as to beneficiaries to receive certain death payments, and to show changes in your family or other personnel listed, for example, as a result of marriage, civil court action, death, or address change.

## INSTRUCTIONS TO CIVILIANS

This extremely important form is to be used by you to show the names and addresses of your spouse, children, parents, and any other person(s) you would like notified if you become a casualty. Not every item on this form is applicable to you. This form is used by the Department of Defense (DoD) to expedite notification in the case of emergencies or death. It does not have a legal impact on other forms you may have completed with the DoD or your employer.

IMPORTANT: This form is divided into two sections: Section 1 - Emergency Contact Information and Section 2 - Benefits Related Information. READ THE INSTRUCTIONS ON PAGES 3 AND 4 BEFORE COMPLETING THIS FORM.

## SECTION 1 - EMERGENCY CONTACT INFORMATION

1. NAME (Last, First, Middle Initial)

MANNING, BRADLEY EDWARD

2. SSN

3a. SERVICE/CIVILIAN CATEGORY

ARMY NAVY MARINE CORPS AIR FORCE DoD CIVILIAN CONTRACTOR

b. REPORTING UNIT CODE/DUTY STATION

WBDA44 / FT DRUM

4a. SPOUSE NAME (if applicable) (Last, First, Middle Initial)

SINGLE

b. ADDRESS (Include ZIP Code) AND TELEPHONE NUMBER

5. CHILDREN

a. NAME (Last, First, Middle Initial)

None.

b. RELATIONSHIP

c. DATE OF BIRTH

(YYYYMMDD)

d. ADDRESS (Include ZIP Code) AND TELEPHONE NUMBER

6a. FATHER NAME (Last, First, Middle Initial)

BRAD EDWARD MANNING

b. ADDRESS (Include ZIP Code) AND TELEPHONE NUMBER

8020 NW 119TH ST (PH: 405-476-1401) OKLAHOMA CITY OK US 73163

7a. MOTHER NAME (Last, First, Middle Initial)

SUSAN MARY MANNING

b. ADDRESS (Include ZIP Code) AND TELEPHONE NUMBER

31 NUBAIN AVE (PH: 011447962069238) HAVERFORDWEST UK

8a. DO NOT NOTIFY DUE TO ILL HEALTH

None.

b. NOTIFY INSTEAD

9a. DESIGNATED PERSON(S) (Military Only)

None.

b. ADDRESS (Include ZIP Code) AND TELEPHONE NUMBER

10. CONTRACTING AGENCY AND TELEPHONE NUMBER (Contractors only)

DD FORM 93 (E), JAN 2008

PREVIOUS EDITION IS OBSOLETE

NAME: MANNING, BRADLEY EDWARD SSN: [REDACTED]

## SECTION 2 - BENEFITS RELATED INFORMATION

11a. BENEFICIARY(IES) FOR DEATH GRATUITY (Military only)

TYLER RAYMOND WATKINS

b. RELATIONSHIP

OTHER

c. ADDRESS (Include ZIP Code) AND TELEPHONE NUMBER

27 ROSS STREET PH: 607-765-6808 OWEGO NY US 13827

d. PERCENTAGE

100

12a. BENEFICIARY(IES) FOR UNPAID PAY/ALLOWANCES (Military only) NAME AND RELATIONSHIP

BRIAN EDWARD MANNING (FATHER)

b. ADDRESS (Include ZIP Code) AND TELEPHONE NUMBER



8020 NW 119TH ST (PH: 405-476-1401) OKLAHOMA CITY OK US 73163

c. PERCENTAGE

100

13a. PERSON AUTHORIZED TO DIRECT DISPOSITION (PADDO)

b. ADDRESS (Include ZIP Code) AND TELEPHONE NUMBER

|   |   |                            |
|---|---|----------------------------|
| NAME: MANNING, BRADLEY EDWARD SSN: [REDACTED]   |   |                            |
| (Military only) NAME AND RELATIONSHIP<br>BRIAN EDWARD MANNING (FATHER)                |   |                            |
| 8020 NW 119TH ST (PH: 405-476-1401) OKLAHOMA CITY OK US 73163                         |   |                            |
| 14. CONTINUATION/REMARKS  |   |                            |
| 15. SIGNATURE OF SERVICE MEMBER/CIVILIAN (Include rank, rate, or grade if applicable) | 16. SIGNATURE OF WITNESS (Include rank, rate or grade as appropriate)   | 17. DATE SIGNED (YYYYMMDD) |
|      |  <i>Nathan R. Rushin SDC</i> | <i>2008021</i>             |

NAME: MANNING, BRADLEY EDWARD SSN: 445989504

## RECORD OF EMERGENCY DATA

## PRIVACY ACT STATEMENT

AUTHORITY: 5 USC 552, 10 USC 555, 1475 to 1480 and 2771, 38 USC 1970, 44 USC 3101, and EO 9397 (SSN).

PRINCIPAL PURPOSES: This form is used by military personnel and Department of Defense civilian and contractor personnel, collectively referred to as civilians, when applicable. For military personnel, it is used to designate beneficiaries for certain benefits in the event of the Service member's death. It is also a guide for disposition of that member's pay and allowances if captured, missing or interned. It also shows names and addresses of the person(s) the Service member desires to be notified in case of emergency or death. For civilian personnel, it is used to expedite the notification process in the event of an emergency and/or death of the member. The purpose of soliciting the SSN is to provide positive identification. All items may not be applicable.

ROUTINE USES: None.

DISCLOSURE: Voluntary; however, failure to provide accurate personal identifier information and other solicited information will delay notification and the processing of benefits to designated beneficiaries if applicable.

## INSTRUCTIONS TO SERVICE MEMBER

This extremely important form is to be used by you to show the names and addresses of your spouse, children, parents, and any other person(s) you would like notified if you become a casualty (other family members or fiancé), and, to designate beneficiaries for certain benefits if you die. IT IS YOUR RESPONSIBILITY to keep your Record of Emergency Data up to date to show your desires as to beneficiaries to receive certain death payments, and to show changes in your family or other personnel listed, for example, as a result of marriage, civil court action, death, or address change.

## INSTRUCTIONS TO CIVILIANS

This extremely important form is to be used by you to show the names and addresses of your spouse, children, parents, and any other person(s) you would like notified if you become a casualty. Not every item on this form is applicable to you. This form is used by the Department of Defense (DoD) to expedite notification in the case of emergencies or death. It does not have a legal impact on other forms you may have completed with the DoD or your employer.

IMPORTANT: This form is divided into two sections: Section 1 - Emergency Contact Information and Section 2 - Benefits Related Information. READ THE INSTRUCTIONS ON PAGES 3 AND 4 BEFORE COMPLETING THIS FORM.

## SECTION 1 - EMERGENCY CONTACT INFORMATION

## 1. NAME (Last, First, Middle Initial)

MANNING, BRADLEY EDWARD

## 2. SSN

## 3a. SERVICE/CIVILIAN CATEGORY

☒ ARMY ☐ NAVY ☐ MARINE CORPS ☐ AIR FORCE ☐ DoD ☐ CIVILIAN ☐ CONTRACTOR

## b. REPORTING UNIT CODE/DUTY STATION

WBDAAA / FT DRUM

## 4a. SPOUSE NAME (if applicable) (Last, First, Middle Initial)

SINGLE

## b. ADDRESS (Include ZIP Code) AND TELEPHONE NUMBER

## 5. CHILDREN

## a. NAME (Last, First, Middle Initial)

None.

## b. RELATIONSHIP

## c. DATE OF BIRTH (YYYYMMDD)

## d. ADDRESS (Include ZIP Code) AND TELEPHONE NUMBER

## 6a. FATHER NAME (Last, First, Middle Initial)

BRIAN EDWARD MANNING

## b. ADDRESS (Include ZIP Code) AND TELEPHONE NUMBER

8020 NW 119TH ST (PH: 405-476-1401) OKLAHOMA CITY OK US 73163

## 7a. MOTHER NAME (Last, First, Middle Initial)

SUSAN MARY MANNING

## b. ADDRESS (Include ZIP Code) AND TELEPHONE NUMBER

31 NUBAIN AVE (PH: 011447962069239) HAVERFORDWEST UK

## 8a. DO NOT NOTIFY DUE TO ILL HEALTH

None.

## b. NOTIFY INSTEAD

## 9a. DESIGNATED PERSON(S) (Military only)

None.

## b. ADDRESS (Include ZIP Code) AND TELEPHONE NUMBER

## 10. CONTRACTING AGENCY AND TELEPHONE NUMBER (Contractors only)

DD FORM 93 (E), JAN 2008

PREVIOUS EDITION IS OBSOLETE

NAME: MANNING, BRADLEY EDWARD SSN: [REDACTED]

## SECTION 2 - BENEFITS RELATED INFORMATION

## 11a. BENEFICIARY(IES) FOR DEATH GRATUITY (Military only)

TYLER RAYMOND WATKINS

## b. RELATIONSHIP

OTHER

## c. ADDRESS (Include ZIP Code) AND TELEPHONE NUMBER

27 ROSS STREET PH: 607-765-6808 OWEGO NY US 13827

100

## 12a. BENEFICIARY(IES) FOR UNPAID PAY/ALLOWANCES (Military only) NAME AND RELATIONSHIP

BRIAN EDWARD MANNING (FATHER)

## b. ADDRESS (Include ZIP Code) AND TELEPHONE NUMBER

8020 NW 119TH ST (PH: 405-476-1401) OKLAHOMA CITY OK US 73163

100

## 13a. PERSON AUTHORIZED TO DIRECT DISPOSITION (PAD)

## b. ADDRESS (Include ZIP Code) AND TELEPHONE NUMBER

## RECORD OF EMERGENCY DATA

Page 2 of 2

NAME: MANNING, BRADLEY EDWARD SSN: 445889504

(Military only) NAME AND RELATIONSHIP

BRIAN EDWARD MANNING (FATHER)

8020 NW 119TH ST (PH: 405-476-1401) OKLAHOMA CITY OK US 73163

## 14. CONTINUATION/REMARKS

15. SIGNATURE OF SERVICE MEMBER/CIVILIAN (Include rank, rate, or grade if applicable)

16. SIGNATURE OF WITNESS (Include rank, rate or grade as appropriate)

17. DATE SIGNED  
(YYYYMMDD)

DD FORM 93 (E) (BACK), JAN 2006

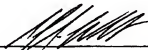
| Please read the instructions before completing this form  |                       |                                   |                     |  |  |
|---|-----------------------|-----------------------------------|---------------------|--|--|
| Servicemembers' Group Life Insurance Election and Certificate   |                       |                                   |                     |  |  |
| Use this form to: (check all that apply)<br><input checked="" type="checkbox"/> Name or update your beneficiary<br>Reduce the amount of your insurance coverage<br>Decline insurance coverage   |                       |                                   |                     | <b>Important:</b> This form is for use by Active Duty and Reserve members. This form does not apply to and cannot be used for any other Government Life Insurance. |  |
| Last name<br>MANNING  | First name<br>BRADLEY | Middle name<br>EDWARD             | Suf.<br>PFC         | Rank, title or grade<br>PFC  | Social Security Number<br>[REDACTED]                   |
| Branch of Service (Do not abbreviate)<br>Army   |                       | Current Duty Location<br>WBDAAA   |                     |  |  |
| <p align="center"><b>Amount of Insurance</b></p> <p>By law, you are automatically insured for \$400,000. <i>If you want \$400,000 of insurance</i>, skip to Beneficiary(ies) and Payment Options. <i>If you want less than \$400,000 of insurance</i>, please check the appropriate block below and write the amount desired and your initials. Coverage is available in increments of \$50,000. <i>If you do not want any insurance</i>, check the appropriate block below and write (in your own handwriting), "I do not want insurance at this time."</p> <p align="center">Declining SGLI coverage also cancels all family coverage under the SGLI program.</p> <p align="center">I want coverage in the amount of \$ _____ Your initials _____</p> <p align="center">(Write "I do not want insurance at this time.")</p> <p><b>*Note:</b> Reduced or refused insurance can only be restored by completing form SGLV 8285 with proof of good health and compliance with other requirements. Reduced or refused insurance will also affect the amount of VGLI you can convert to upon separation from service.</p> |                       |                                   |                     |  |  |
| <b>Beneficiary(ies) and Payment Options</b>   |                       |                                   |                     |  |  |
| I designate the following beneficiary(ies) to receive payment of my insurance proceeds. I understand that the principal beneficiary(ies) will receive payment upon my death. If all principal beneficiaries predecease me, the insurance will be paid to the contingent beneficiary(ies).   |                       |                                   |                     |  |  |
| Complete Name (first, middle, last) and Address of each beneficiary   |                       | Social Security Number (If known) | Relationship to you | Share to each beneficiary (Use %, \$ amounts or fractions)   | Payment Option (Lump sum or 36 equal monthly payments) |
| Principal<br>1. TYLER RAYMOND WATKINS 27 ROSS STREET PH: 607-765-6808 OWEGO NY US 13827   |                       |                                   | OTHER               | 100%   | LUMP SUM   |
| Contingent<br>1. DEBRA VAN ALSTYNE 1442 SELWORTHY ROAD PH: 301-739-7816 POTOMAC MD US 20854   |                       |                                   | AUNT                | 100%   | LUMP SUM   |
| I HAVE READ AND UNDERSTAND the instructions on pages 2 and 3 of this form. I ALSO UNDERSTAND that: <ul style="list-style-type: none"> <li>This form cancels any prior beneficiary or payment instructions.</li> <li>The proceeds will be paid to beneficiaries as stated in #6 on page 3 of this form, unless otherwise stated above.</li> <li>If I have legal questions about this form, I may consult with a military attorney at no expense to me.</li> <li>I cannot have combined SGLI and VGLI coverages at the same time for more than \$400,000.</li> </ul>  |                       |                                   |                     |  |  |
| SIGN HERE IN INK<br>(Your Signature. Do not print.)   |                       |                                   | Date: 20090821      |  |  |
| Do not write in space below. For official use only.   |                       |                                   |                     |  |  |
| WITNESSED AND RECEIVED BY:  |                       | RANK, TITLE OR GRADE              | ORGANIZATION        | DATE RECEIVED  |  |
| [Signature]   |                       | SPE                               | 2ND BCT 3DE         | 20090821   |  |
| SGLV-8286 (E)   |                       |                                   |                     |  |  |



DEPARTMENT OF THE ARMY  
**CERTIFICATE OF TRAINING**

This is to certify that  
**PV2 BRADLEY MANNING** 445-98-9504  
has successfully completed  
**Combat Lifesavers Course 40 HRS**

Given at 26 SEPT 2008

  
\_\_\_\_\_  
PAUL R. WALTER  
LTC, MI  
Commanding

| Please read the instructions before completing this form   |                                   |                                 |   |  |                                      |   |                                   |                     |  |  |  |  |        |      |          |
|--|-----------------------------------|---------------------------------|---|--|--------------------------------------|---|-----------------------------------|---------------------|--|--|--|--|--------|------|----------|
| Servicemembers' Group Life Insurance Election and Certificate  |                                   |                                 |   |  |                                      |   |                                   |                     |  |  |  |  |        |      |          |
| Use this form to: (check all that apply)   |                                   |                                 | Important: This form is for use by Active Duty and Reserve members. This form does not apply to and cannot be used for any other Government Life Insurance. |  |                                      |   |                                   |                     |  |  |  |  |        |      |          |
| <input checked="" type="checkbox"/> Name or update your beneficiary<br><input type="checkbox"/> Reduce the amount of your insurance coverage<br><input type="checkbox"/> Decline insurance coverage  |                                   |                                 |   |  |                                      |   |                                   |                     |  |  |  |  |        |      |          |
| Last name<br>MANNING   | First name<br>BRADLEY             | Middle name<br>EDWARD           | Suf   | Rank, title or grade<br>PV2                            | Social Security Number<br>[REDACTED] |   |                                   |                     |  |  |  |  |        |      |          |
| Branch of Service(Do not abbreviate)<br>Army   |                                   | Current Duty Location<br>WBDAA8 |   |  |                                      |   |                                   |                     |  |  |  |  |        |      |          |
| <p align="center"><b>Amount of Insurance</b></p> <p>By law, you are automatically insured for \$400,000. If you want \$400,000 of insurance, skip to Beneficiary(ies) and Payment Options. If you want less than \$400,000 of insurance, please check the appropriate block below and write the amount desired and your initials. Coverage is available in increments of \$50,000. If you do not want any insurance, check the appropriate block below and write (in your own handwriting). "I do not want insurance at this time."</p> <p align="center">Declining SGLI coverage also cancels all family coverage under the SGLI program.</p> <p><input type="checkbox"/> I want coverage in the amount of \$ _____ Your Initials _____</p> <p align="center">(While "I do not want insurance at this time.")</p> <p><small>*Note: Reduced or refused insurance can only be restored by completing form SGLV 8285 with proof of good health and compliance with other requirements. Reduced or refused insurance will also affect the amount of VGLI you can convert to upon separation from service.</small></p> |                                   |                                 |   |  |                                      |   |                                   |                     |  |  |  |  |        |      |          |
| <p align="center"><b>Beneficiary(ies) and Payment Options</b></p> <p>I designate the following beneficiary(ies) to receive payment of my insurance proceeds. I understand that the principal beneficiary(ies) will receive payment upon my death. If all principal beneficiaries predecease me, the insurance will be paid to the contingent beneficiary(ies).</p> <table border="1"> <thead> <tr> <th>Complete Name (first, middle, last) and Address of each beneficiary</th> <th>Social Security Number (if known)</th> <th>Relationship to you</th> <th>Share to each beneficiary (Use % 5 amounts or fractions)</th> <th>Payment Option (Lump sum or 36 equal monthly payments)</th> </tr> </thead> <tbody> <tr> <td>Principal<br/>1. BRIAN EDWARD MANNING 8020 NW 119TH ST (PH: 405-476-1401) OKLAHOMA CITY OK US 73163<br/>Contingent</td> <td></td> <td>FATHER</td> <td>100%</td> <td>LUMP SUM</td> </tr> </tbody> </table>  |                                   |                                 |   |  |                                      | Complete Name (first, middle, last) and Address of each beneficiary | Social Security Number (if known) | Relationship to you | Share to each beneficiary (Use % 5 amounts or fractions) | Payment Option (Lump sum or 36 equal monthly payments) | Principal<br>1. BRIAN EDWARD MANNING 8020 NW 119TH ST (PH: 405-476-1401) OKLAHOMA CITY OK US 73163<br>Contingent |  | FATHER | 100% | LUMP SUM |
| Complete Name (first, middle, last) and Address of each beneficiary  | Social Security Number (if known) | Relationship to you             | Share to each beneficiary (Use % 5 amounts or fractions)  | Payment Option (Lump sum or 36 equal monthly payments) |                                      |   |                                   |                     |  |  |  |  |        |      |          |
| Principal<br>1. BRIAN EDWARD MANNING 8020 NW 119TH ST (PH: 405-476-1401) OKLAHOMA CITY OK US 73163<br>Contingent   |                                   | FATHER                          | 100%  | LUMP SUM   |                                      |   |                                   |                     |  |  |  |  |        |      |          |
| <p>I HAVE READ AND UNDERSTAND the instructions on pages 2 and 3 of this form. I ALSO UNDERSTAND that:</p> <ul style="list-style-type: none"> <li>This form cancels any prior beneficiary or payment instructions.</li> <li>The proceeds will be paid to beneficiaries as stated in #6 on page 3 of this form, unless otherwise stated above.</li> <li>If I have legal questions about this form, I may consult with a military attorney at no expense to me.</li> <li>I cannot have combined SGLI and VGLI coverages at the same time for more than \$400,000.</li> </ul>  |                                   |                                 |   |  |                                      |   |                                   |                     |  |  |  |  |        |      |          |
| SIGN HERE IN INK   |                                   |                                 | Date: 20080902  |  | Be M                                 |   |                                   |                     |  |  |  |  |        |      |          |
| (Your Signature, Do not print)   |                                   |                                 |   |  |                                      |   |                                   |                     |  |  |  |  |        |      |          |
| Do not write in spaces below. For official use only.   |                                   |                                 |   |  |                                      |   |                                   |                     |  |  |  |  |        |      |          |
| WITNESSED AND RECEIVED BY:   |                                   | RANK, TITLE OR GRADE            | ORGANIZATION  | DATE RECEIVED  |                                      |   |                                   |                     |  |  |  |  |        |      |          |
| [Signature]  |                                   | PV2                             | PSDR  | 20080902   |                                      |   |                                   |                     |  |  |  |  |        |      |          |
| SGLV-8285 (E)  |                                   |                                 |   |  |                                      |   |                                   |                     |  |  |  |  |        |      |          |

AN AGREEMENT BETWEEN

**BRADLEY EDWARD MANNING**

AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12356, or under any other Executive order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Sections 1.1 and 1.2(e) of Executive Order 12356, or under any other Executive order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

3. I have been advised that the unauthorized disclosure, unauthorized retention, or negligent handling of classified information by me could cause damage or irreparable injury to the United States or could be used to advantage by a foreign nation. I hereby agree that I will never divulge classified information to anyone unless: (a) I have officially verified that the recipient has been properly authorized by the United States Government to receive it; or (b) I have been given prior written notice of authorization from the United States Government Department or Agency (hereinafter Department or Agency) responsible for the classification of the information or last granting me a security clearance that such disclosure is permitted. I understand that if I am uncertain about the classification status of information, I am required to confirm from an authorized official that the information is unclassified before I may disclose it, except to a person as provided in (a) or (b), above. I further understand that I am obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearances I hold; removal from any position of special confidence and trust requiring such clearances; or the termination of my employment or other relationships with the Departments or Agencies that granted my security clearance or clearances. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation, or violations, of United States criminal laws, including the provisions of Sections 641, 793, 794, 798, and \*952, Title 18, United States Code, \*the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication, or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Section 793, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.


9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

(Continue on reverse.)



11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this Agreement and its implementing regulation (32 CFR Section 2003.20) so that I may read them at this time, if I so choose.

|   |                   |   |
|---|-------------------|---|
| SIGNATURE<br> | DATE<br>07 APR 08 | SOCIAL SECURITY NUMBER<br>(See Notice below)<br>445 98 9504 |
|---|-------------------|---|

ORGANIZATION OF CONTRACTOR, LICENSEE, GRANTEE OR AGENT, PROVIDE: NAME, ADDRESS, AND, IF APPLICABLE, FEDERAL SUPPLY CODE NUMBER)  
(Type or Print)

Company: D CO  
Battalion: 305TH MI BN  
Fort Huachuca, Arizona 85613

Attestation completed on: 07 APR 08

| WITNESS  |             | ACCEPTANCE   |             |
|--|-------------|--|-------------|
| THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED.  |             | THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.                       |             |
| SIGNATURE  | DATE        | SIGNATURE  | DATE        |
| Elisa K. Rubin   | 07 APR 2008 | Elisa K. Rubin   | 07 APR 2008 |
| NAME AND ADDRESS (Type or print)   |             | NAME AND ADDRESS (Type or print)   |             |
| Commander, USAIC&FH<br>ATTN: ATZS-GI-E<br>Building # 22320, Augur Avenue<br>Fort Huachuca, AZ 85613-6000 |             | Commander, USAIC&FH<br>ATTN: ATZS-GI-E<br>Building # 22320, Augur Avenue<br>Fort Huachuca, AZ 85613-6000 |             |

#### SECURITY DEBRIEFING ACKNOWLEDGMENT

I reaffirm that the provisions of the espionage laws, other federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I (have) (have not) (strike out inappropriate word or words) received a security debriefing.

|                                 |                      |
|---------------------------------|----------------------|
| SIGNATURE OF EMPLOYEE           | DATE                 |
| NAME OF WITNESS (Type or print) | SIGNATURE OF WITNESS |

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Account Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access to the information indicated above or 2) determine that your access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations, or possibly result in the denial of your being granted access to classified information.

\* NOT APPLICABLE TO NON-GOVERNMENT PERSONNEL SIGNING THIS AGREEMENT.

STANDARD FORM 312 BACK (REV. 1-91)

USAPPC V2.00

07275B1010

## MONTGOMERY GI BILL ACT OF 1984 (MGIB)

(Chapter 30, Title 38, U.S. Code)

## BASIC ENROLLMENT

## PRIVACY ACT STATEMENT

AUTHORITY: Chapter 30, Title 38, U.S. Code, Sections 3011, 3012, 3018A, and 3018B; and EO 9397.

PRINCIPAL PURPOSE: To document the understanding of members about their eligibility or lack of eligibility for benefits under the Montgomery GI Bill Act of 1984 (MGIB) and document a member's election to decline enrollment for benefits under the MGIB.

ROUTINE USES: To the Department of Veterans' Affairs to ascertain an individual's eligibility to claim benefits under the MGIB.

DISCLOSURE: Voluntary; however, failure to provide the requested information will result in the individual being automatically enrolled in the MGIB program.

## 1. SERVICE MEMBER DATA

a. NAME (LAST, First, Middle Initial)

MANNING BRADLEY E

b. SOCIAL SECURITY NUMBER (SSN)

## 2. STATEMENT OF UNDERSTANDING FOR INELIGIBLE MEMBERS

I am NOT eligible for MGIB because (a) I am a Service Academy graduate, or (b) I am an ROTC scholarship graduate who received more than the current minimum amount allowed for enrollment in MGIB, or (c) I am a prior service member who disenrolled during my previous term of active duty.

(1) SERVICE MEMBER SIGNATURE

(2) RANK / GRADE

(3) DATE SIGNED (YYYYMMDD)

## 3. STATEMENT OF UNDERSTANDING FOR ALL ELIGIBLE MEMBERS

(1) I am automatically enrolled unless I exercise the option to **DISENROLL** by signing item 5 below.(2) **UNLESS I DISENROLL** from the MGIB, my basic pay will be reduced \$100 per month or the current monthly rate until \$1,200 has been deducted; this basic pay reduction **CANNOT** be REFUNDED, SUSPENDED OR STOPPED, this is an **IRREVOCABLE DECISION**.

(3) I must complete 36 months of active duty service (24 months if my enlistment is for less than 36 months) before I am entitled to the current rate of monthly benefits. The MGIB provides benefits for a period of 36 months.

(4) I understand I am eligible for an increased monthly benefit by contributing an additional amount, not to exceed \$600 while on active duty. Once I separate, I cannot contribute.

(5) I must receive an **HONORABLE** discharge for service establishing entitlement to the MGIB. This **DOES NOT** include "under honorable conditions."

(6) I must complete the requirements of a secondary school diploma or equivalency certification, or successfully complete the equivalent of 12 semester hours in a program of education leading to a standard college degree before applying for benefits with the Department of Veterans' Affairs.

(7) I have 10 years from date of last discharge from active duty to use MGIB benefits.

(8) If I die while on active duty, or within one year after discharge or release from active duty if service related, my designated beneficiary(ies) will receive the unused balance of the money reduced from my basic pay for the MGIB. This death benefit will be paid by the Department of Veterans' Affairs (DVA).

(9) I cannot receive any combination of DVA educational benefits in excess of 48 months.

(10) I must complete at least 24 months of a 3 year active duty service obligation and if my obligation is 2 years I may join and serve honorably in the Selected Reserve for a minimum of 48 months to qualify for the current active duty benefit rate. A (one) period of service **CANNOT** qualify me for both active and reserve MGIB benefits.

(a) SERVICE MEMBER SIGNATURE

X

(b) RANK/GRADE

PV1/E01

(c) DATE SIGNED (YYYYMMDD)

20071004

## 4. SERVICE UNIQUE EDUCATION ASSISTANCE OPTIONS

MOS SSP

TOS 4YRS

CASH BONUS

## 5. STATEMENT OF DISENROLLMENT

I DO NOT desire to participate in the MGIB. I understand the benefits of the MGIB program and that I WILL NOT be able to enroll at a later date.

a. DATE SIGNED  
(YYYYMMDD)

b. RANK/GRADE

c. SERVICE MEMBER SIGNATURE

## 6. CERTIFYING OFFICIAL

a. TYPED OR PRINTED NAME (LAST, First, Middle Initial)

MURPHY VENA

b. RANK/GRADE

GS-4

c. SIGNATURE

d. DATE SIGNED

(YYYYMMDD)

20071004

**Office of Personnel Management**

EPSQ version

2.2

**SECURITY CLEARANCE APPLICATION**

O.M.B. No. 3206-0007

Date: 10/04/2007

Time: 10:14

AM

Standard Form 86, Sep. 95

Manning, Bradley Edward

SSN: [REDACTED]

---

**1. Personal Information****Name:** Manning

Bradley Edward

**Birth Date:** 1987/12/17**Sex:**

MALE

**Place of Birth:** Oklahoma City, OK**County:** OKLAHOMA

UNITED STATES

**Maiden Name:****Work/Day Phone:****Home/Evening Phone:** 301-738-

7816

**Height:** 5 - 2**Weight:** 101.00**Hair Color:** BLOND**Eye Color:**

BLUE

---

**2. Other Names Used**

NO Have you ever used or been known by another name?

---

**3. Citizenship****Current Citizenship:** U.S. CITIZEN AT BIRTH, NATIVE BORN**Mothers Maiden Name:** Fox

Susan Mary

NO Are you now or were you a dual citizen of the U.S. and another country?

**Passport Number:** 711133054  
2005/08/24**Passport Issuance Date:**

---

**4. Where You Have Lived****FROM****TO****ADDRESS**  
-----

1. 2006/07/10

PRES

1492 Selworthy Road  
Potomac, MD 20854

**Person Who Knows You:**

Girardi, Mary Rey  
1494 Selworthy Road  
Potomac, MD 20854  
**Phone:** 011 301-351-3522

**NO** Is this residence address hard to find?

2. 2006/04/10      2006/07/09      5607 71st Place East APT 1005  
Tulsa, OK 74136

**Person Who Knows You:**

Davis, Jill Elizabeth  
5502 E 71st Place East  
Tulsa, OK 74136  
**Phone:** 011 918-728-8511

**NO** Is this residence address hard to find?

3. 2005/09/10      2006/04/09      8020 NW 119th Street  
Oklahoma City, OK 73162

**Person Who Knows You:**

Davis, David Scott  
5502 E 71ST Place East  
Tulsa, OK 74136  
**Phone:** 011 918-728-8511

**NO** Is this residence address hard to find?

4. 2001/11/10      2005/09/09      31 Nubian Ave  
Haverford, UNITED KINGDOM 61142

**Person Who Knows You:**

Weir, David John  
217 Shortgrass Road  
Edmond, OK 73003  
**Phone:** 011 405-715-0388

**NO** Is this residence address hard to find?

5. 1992/01/09      2001/11/09      216 E Adams Street  
Crescent, OK 73028

**Person Who Knows You:**

Egelston, Mary Ann  
RT 1 Box 11 R2  
Crescent, OK 73028

Phone: 011 405-964-2929

NO Is this residence address hard to find?

---

## 5. Where You Went To School

YES Have you attended school beyond Junior High School within the last 5 years?

| FROM  | TO         | TYPE/ADDRESS   |
|---|------------|--|
| -----   |            |  |
| 1. 2001/09/01   | 2005/06/09 | HIGH SCHOOL  |
| <b>Degree/Diploma/Other</b><br>HIGH SCHOOL DIPLOMA  |            | Tasker Milward VC  |
| <b>Award Date:</b> 2005/06/09   |            | Portfield Ave Haverford<br>Wales, UNITED KINGDOM SA611EQ |
| <b>Person Who Knows You</b><br>Weir, Carrol NMN<br>217 Shortgrass Road<br>Edmond, OK 73003<br><b>Phone:</b> 011 405-715-0388    |            |  |
| 2. 2007/01/09   | 2007/05/10 | COLLEGE, UNIVERSITY, MILITARY                            |
| COLLEGE   |            |  |
| <b>Degree/Diploma/Other</b><br>ROCKVILLE  |            | MONTGOMERY COLLEGE OF                                    |
| <b>Award Date:</b>  |            | 51 Mannakee St<br>Rockville, MD 20850-1101               |
| <b>Person Who Knows You</b><br>Hessam, Aram NMN<br>51 Mannakee St<br>Rockville, MD 20850-1101<br><b>Phone:</b> 011 240-567-7277 |            |  |

---

## 6. Your Employment Activities

| FROM          | TO   | TYPE OF EMPLOYMENT |
|---------------|------|--------------------|
| -----         |      |                    |
| 1. 2007/01/10 | PRES | OTHER              |

**Your Position:** Barista  
**Employer Name:** Starbucks  
**Employer Address:** 7911 Tuckerman Lane  
Potomac, MD 20854  
**Employer Phone:** 011 301-765-0556

**Supervisor Name:** Rubin  
David Mark  
**Supervisor Phone:**

**NO** Is the job address different from the employer's address?

**NO** Is the supervisor's address different from the job location address?

**PREVIOUS PERIODS OF ACTIVITY:**

**NO** Have you worked for this organization previously?

2. 2006/06/10      2007/01/09      UNEMPLOYMENT (INCLUDE NAME OF  
PERSON WHO CAN      VERIFY)

**Your Position:** Unemployed  
**Employer Name:** Mary Girardi  
**Employer Address:** 1492 Selworthy  
Potomac, MD 20854  
**Employer Phone:** 011 301-738-7816

3. 2006/04/10      2006/06/09      OTHER

**Your Position:** Asst Manager  
**Employer Name:** FYE  
**Employer Address:** 7021 S Memorial Drive  
Tulsa, OK 74133  
**Employer Phone:** 011 918-252-7399

**Supervisor Name:** Stewart  
Rodney James  
**Supervisor Phone:**

**NO** Is the job address different from the employer's address?

**NO** Is the supervisor's address different from the job location address?

**PREVIOUS PERIODS OF ACTIVITY:**

**NO** Have you worked for this organization previously?

4. 2006/02/10 2006/04/09 OTHER

**Your Position:** Intern Programmer  
**Employer Name:** Zoto Inc  
**Employer Address:** 123 South Hudson Street  
Oklahoma City, OK 73102  
**Employer Phone:** 011 650-641-0108

**Supervisor Name:** Campbell  
Thomas Kord  
**Supervisor Phone:**

NO Is the job address different from the employer's address?

NO Is the supervisor's address different from the job location address?

**PREVIOUS PERIODS OF ACTIVITY:**

NO Have you worked for this organization previously?

5. 2005/09/10 2006/02/09 OTHER

**Your Position:** Server  
**Employer Name:** Incredible Pizza Co  
**Employer Address:** 8314 E 71St  
Tulsa, OK 74133  
**Employer Phone:** 011 918-294-8671

**Supervisor Name:** Edwards  
John Brad  
**Supervisor Phone:**

NO Is the job address different from the employer's address?

NO Is the supervisor's address different from the job location address?

**PREVIOUS PERIODS OF ACTIVITY:**

NO Have you worked for this organization previously?

6. 1988/08/03 2005/09/09 UNEMPLOYMENT (INCLUDE NAME OF  
PERSON WHO CAN VERIFY)

**Your Position:** Unemployed  
**Employer Name:** Susan Fox  
**Employer Address:** 31 Nubian Ave

Haverford, MD 20854  
**Employer Phone:** 011 301-668-5610

NO Were you in the Federal Civil Service prior to the last 10 years?

---

**7. People Who Know You Well**

|    | FROM       | TO   | REFERENCE NAME/ADDRESS   |
|----|------------|------|--|
|    | -----      |      |  |
|    | -----      |      |  |
| 1. | 1996/01/14 | PRES | Radford<br>Thomas Paden<br><b>Home Address:</b> Trailer 28 4701 East Coffee Creek<br>Road<br><b>Evening Phone:</b> Edmond OK 73034<br>011 405-744-6384 |
| 2. | 1993/09/10 | PRES | Radford<br>Mark Allen<br><b>Home Address:</b> 18 Lakeview Drive<br>Cresent OK 73028<br><b>Evening Phone:</b> 011 405-280-7434                          |
| 3. | 1993/08/10 | PRES | Davis<br>Jordan Scott<br><b>Home Address:</b> Trail 28 4701 Coffee Creek Road<br>Edmond OK 73034<br><b>Evening Phone:</b> 011 918-946-5121             |

---

**8. Your Spouse**

**What is your current marital status?** NEVER MARRIED

---

**9. Your Relatives and Associates**

| RELATIONSHIP | NAME/ADDRESS |
|--------------|--------------|
| -----        |              |
| -----        |              |
| 1. MOTHER    | Fox          |



Susan Mary  
31 Nubian Ave  
Haverford West, UNITED KINGDOM

SA611HS

DOB: 1953/08/10

POB: UNITED KINGDOM

Country of Citizenship: UNITED KINGDOM

2. FATHER

Manning  
Brian Edward  
8020 NW 119th Street  
Oklahoma City 73103

DOB: 1955/07/22

POB: UNITED STATES

Country of Citizenship: UNITED STATES

3. SISTER

Major  
Casey Manning  
308 NW 24th ST  
Oklahoma City 73103

DOB: 1976/12/17

POB: UNITED STATES

Country of Citizenship: UNITED STATES

---

## 10. Citizenship of Your Relatives and Associates

| RELATIONSHIP | NAME |
|--------------|------|
|--------------|------|

1. MOTHER

DOB: 1953/08/10

Fox

Susan Mary

Type: OTHER

Citz. Date:

Certificate Number:

Court:

City/State:

Comments: Mother is not a citizen of the United States but is a citizen of the UK.

---

## 11. Your Military History

NO Have you ever served in the military? (If yes, provide in chronological order your military history: begin with the most recent period and include Reserves, National Guard, Merchant Marines, and Foreign Military Service.)

---

## INSTRUCTIONS FOR PREPARING AND ARRANGING RECORD OF TRIAL

**USE OF FORM** - Use this form and MCM, 1984, Appendix 14, will be used by the trial counsel and the reporter as a guide to the preparation of the record of trial in general and special court-martial cases in which a verbatim record is prepared. Air Force uses this form and departmental instructions as a guide to the preparation of the record of trial in general and special court-martial cases in which a summarized record is authorized.

Army and Navy use DD Form 491 for records of trial in general and special court-martial cases in which a summarized record is authorized. Inapplicable words of the printed text will be deleted.

**COPIES** - See MCM, 1984, RCM 1103(g). The convening authority may direct the preparation of additional copies.

**ARRANGEMENT** - When forwarded to the appropriate Judge Advocate General or for judge advocate review pursuant to Article 64(a), the record will be arranged and bound with allied papers in the sequence indicated below. Trial counsel is responsible for arranging the record as indicated, except that items 6, 7, and 15e will be inserted by the convening or reviewing authority, as appropriate, and items 10 and 14 will be inserted by either trial counsel or the convening or reviewing authority, whichever has custody of them.

1. Front cover and inside front cover (chronology sheet) of DD Form 490.

2. Judge advocate's review pursuant to Article 64(a), if any.

3. Request of accused for appellate defense counsel, or waiver/withdrawal of appellate rights, if applicable.

4. Briefs of counsel submitted after trial, if any (Article 38(c)).

5. DD Form 494, "Court-Martial Data Sheet."

6. Court-martial orders promulgating the result of trial as to each accused, in 10 copies when the record is verbatim and in 4 copies when it is summarized.

7. When required, signed recommendation of staff judge advocate or legal officer, in duplicate, together with all clemency papers, including clemency recommendations by court members.

8. Matters submitted by the accused pursuant to Article 60 (MCM, 1984, RCM 1105).

9. DD Form 458, "Charge Sheet" (unless included at the point of arraignment in the record).

10. Congressional inquiries and replies, if any.

11. DD Form 457, "Investigating Officer's Report," pursuant to Article 32, if such investigation was conducted, followed by any other papers which accompanied the charges when referred for trial, unless included in the record of trial proper.

12. Advice of staff judge advocate or legal officer, when prepared pursuant to Article 34 or otherwise.

13. Requests by counsel and action of the convening authority taken thereon (e.g., requests concerning delay, witnesses and depositions).

14. Records of former trials.

15. Record of trial in the following order:

a. Errata sheet, if any.

b. Index sheet with reverse side containing receipt of accused or defense counsel for copy of record or certificate in lieu of receipt.

c. Record of proceedings in court, including Article 39(a) sessions, if any.

d. Authentication sheet, followed by certificate of correction, if any.

e. Action of convening authority and, if appropriate, action of officer exercising general court-martial jurisdiction.

f. Exhibits admitted in evidence.

g. Exhibits not received in evidence. The page of the record of trial where each exhibit was offered and rejected will be noted on the front of each exhibit.

h. Appellate exhibits, such as proposed instructions, written offers of proof or preliminary evidence (real or documentary), and briefs of counsel submitted at trial.